Novell® Sentinel™

5.1.3

www.novell.com

Volume III – GUIDA DELL'UTENTE DI SENTINEL WIZARD

7 luglio 2006

Novell®

Marchi di fabbrica Novell

Per i marchi Novell, vedere l'elenco disponibile all'indirizzo
http://www.novell.com/company/legal/trademarks/tmlist.html.

Materiali di terze parti

Tutti i marchi di fabbrica di terze parti appartengono ai rispettivi proprietari.

Note legali di terze parti

In Sentinel 5 possono essere incluse le tecnologie di terze parti seguenti:

- Apache Axis e Apache Tomcat, Copyright © 1999-2005, Apache Software Foundation. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.apache.org/licenses/
- ANTLR. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.antlr.org
- Boost, Copyright © 1999, Boost.org.
- Bouncy Castle, Copyright © 2000-2004, the Legion of Bouncy Castle. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.bouncycastle.org.
- Checkpoint. Copyright © Check Point Software Technologies Ltd.
- Concurrent, pacchetto di utility. Copyright © Doug Lea. Utilizzato senza classi CopyOnWriteArrayList e ConcurrentReaderHashMap.
- Crypto++ Compilation. Copyright © 1995-2003, Wei Dai, con i materiali protetti da copyright seguenti: mars. cpp di Brian Gladman e Sean Woods. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.eskimo.com/~weidai/License.txt.
- Crystal Reports Developer e Crystal Reports Server. Copyright © 2004 Business Objects Software Limited.
- DataDirect Technologies Corp. Copyright © 1991-2003.
- edpFTPj, concesso in licenza in base alla GNU Lesser General Public License. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Enhydra Shark, concesso in licenza in base alla Lesser General Public License disponibile all'indirizzo: http://shark.objectweb.org/license.html.
- ICEsoft ICEbrowser. ICEsoft Technologies, Inc. Copyright © 2003-2004.
- ILOG, Inc. Copyright © 1999-2004.
- Installshield Universal. Copyright © 1996-2005, Macrovision Corporation e/o Macrovision Europe Ltd.
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare il sito Web all’indirizzo http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt (in lingua inglese).

  Java 2 Platform può inoltre includere i prodotti di terze parti seguenti:

  - CoolServlets © 1999
  - DES and 3xDES © 2000 by Jef Poskanzer
  - Crimson © 1999-2000 The Apache Software Foundation
  - Xalan J2 © 1999-2000 The Apache Software Foundation
  - NSIS 1. 0j © 1999-2000 Nullsoft, Inc.
  - Eastman Kodak Company © 1992

Sommario

Prefazione

La documentazione tecnica di Sentinel contiene informazioni generali sull'utilizzo e rappresenta una guida di riferimento. La presente documentazione č rivolta ai responsabili della protezione delle informazioni. Il testo contenuto nella presente documentazione č da considerarsi come documento di riferimento del sistema di gestione della protezione aziendale di Sentinel. Sul portale Web di Sentinel sono disponibili altri documenti.

La documentazione tecnica di Sentinel č suddivisa in cinque differenti volumi, ovvero:

- Volume I: Guida all'installazione di Sentinel™ 5
- Volume II: Guida dell'utente di Sentinel™ 5
- Volume III: Guida dell'utente di Sentinel™ 5 Wizard
- Volume IV: Guida di riferimento dell'utente di Sentinel™ 5
- Volume V: Guida all'integrazione di terze parti di Sentinel™

Volume I: Guida all'installazione di Sentinel 5

In questa guida viene descritto come installare i prodotti seguenti:

- Server Sentinel
- Console Sentinel
- Motore di correlazione di Sentinel
- Crystal Reports per Sentinel
- Generatore servizi di raccolta di Wizard
- Gestione servizi di raccolta di Wizard
- Advisor

Volume II: Guida dell'utente di Sentinel

In questa guida vengono descritti gli argomenti seguenti:

- Funzionamento della console Sentinel
- Funzioni di Sentinel
- Architettura di Sentinel
- Comunicazione di Sentinel
- Arresto/Avvio di Sentinel
- Valutazione delle vulnerabilitŕ
- Monitoraggio degli eventi
- Filtraggio degli eventi
- Correlazione degli eventi
- Gestione dati Sentinel
- Configurazione eventi per rilevanza aziendale
- Servizio di mappatura
- Rapporti cronologici
- Gestione di host Wizard
- Casi
- Situazioni
- Gestione utenti
- Workflow

Volume III: Guida dell'utente di Wizard

In questa guida vengono descritti gli argomenti seguenti:

- Funzionamento della procedura guidata Generatore servizi di raccolta
- Gestione servizi di raccolta di Wizard
- servizi di raccolta
- Gestione di host Wizard
- Creazione e manutenzione dei servizi di raccolta

Volume IV: Guida di riferimento dell'utenti di Sentinel

In questa guida vengono descritti gli argomenti seguenti:

- Linguaggio di script di Wizard
- Comandi di analisi sintattica di Wizard
- Funzioni dell'amministratore di Wizard
- Tag META di Wizard e Sentinel
- Motore di correlazione di Sentinel
- Autorizzazioni utente
- Opzioni della riga di comando di correlazione
- Schema database Sentinel

Volume V: Guida all'integrazione di soluzioni di terze parti di Sentinel

- Remedy
- Operazioni di HP OpenView
- HP Service Desk

1 Introduzione a Wizard

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

La Guida dell'utente di Wizard costituisce un'introduzione al funzionamento di Novell Wizard. In questa guida viene illustrato ogni componente e il relativo funzionamento.

In questa guida si presume che l'utente abbia familiarità con la sicurezza di rete, l'amministrazione dei database e i sistemi operativi Windows e UNIX.

Sommario

Questa guida contiene i capitoli seguenti:

- Capitolo 1: Introduzione a Wizard
- Capitolo 2: Gestione di host Wizard
- Capitolo 3: Creazione e manutenzione dei servizi di raccolta
- Appendice A: Connettore syslog
- Appendice B: Server socket
- Appendice C: Informazioni sul copyright

Convenzioni utilizzate

Note e avvertenze

NOTA: le Note forniscono ulteriori informazioni che possono rivelarsi utili.

ATTENZIONE: le avvertenze forniscono ulteriori informazioni che possono essere utili per evitare danni al sistema o perdite di dati.

Comandi

I comandi sono visualizzati con il font courier. Ad esempio:

```
useradd -g dba -d /export/home/oracle -m -s /bin/csh
   oracle
```

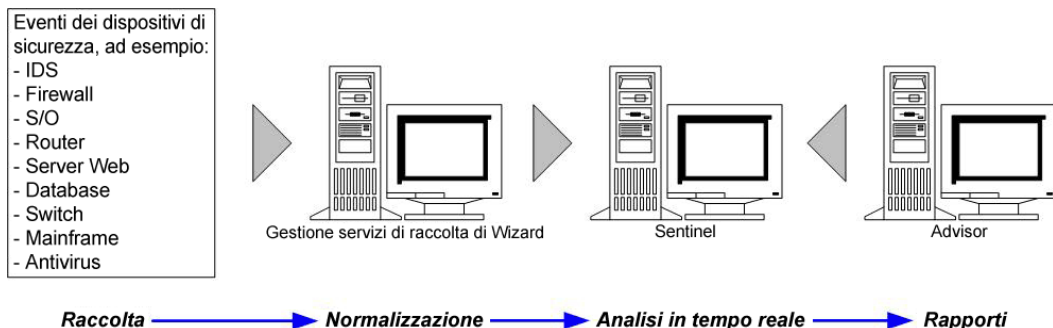
Wizard

Sentinel Wizard consente di creare, configurare e controllare i servizi di raccolta. I servizi di raccolta sono utilizzati per raccogliere e normalizzare gli eventi generati dai dispositivi e dai programmi di sicurezza. Gli eventi normalizzati vengono quindi inviati a Sentinel affinché li utilizzi per correlare analisi, generare report e rispondere ai casi in tempo reale.

NOTA: sebbene non sia obbligatorio, è consigliabile che in una configurazione che preveda più istanze di Generatore servizi di raccolta di Wizard una di esse sia indicata come principale. Il computer in questione viene pertanto utilizzato per memorizzare, sviluppare o modificare i servizi di raccolta nonché per configurare porte.

Wizard è costituito dai componenti seguenti:

- Generatore servizi di raccolta è l'interfaccia utente di Wizard che consente di creare, configurare, distribuire e controllare i servizi di raccolta. Oltre che per eseguire i servizi di raccolta a livello locale, è possibile utilizzare il generatore per caricare, scaricare e controllare questi ultimi nei sistemi remoti.
- Gestione servizi di raccolta): è il componente back-end di Wizard che gestisce i servizi di raccolta e i messaggi di stato del sistema ed esegue il filtro globale degli eventi.

Un Servizio di raccolta raccoglie e normalizza gli eventi non elaborati da programmi e dispositivi di sicurezza e fornisce in output eventi normalizzati che possano essere correlati, segnalati e utilizzati per rispondere ai casi. Il software Sentinel viene fornito con servizi di raccolta di livello 1. Per scaricare ulteriori servizi di raccolta, visitare il portale del servizio clienti all'indirizzo http://www.esecurityinc.com/ (in lingua inglese).

Servizi di raccolta

Il servizi di raccolta sono utilizzati per filtrare e normalizzare i dati relativi a eventi importanti, convertirli in un formato standard e metterli a disposizione del processo di Sentinel. Esistono tre livelli di servizi di raccolta, ovvero:

- servizi di raccolta supportati (T1), che:
  - sono documentati
  - dispongono di metadati
  - sono disponibili per tutti i clienti
  - Supporto tecnico
- Servizi di raccolta documentati (T2), che:
  - sono destinati alla libreria dei servizi di raccolta
  - sono documentati
  - dispongono di metadati
  - si basano sui modelli standard di Sentinel
  - Supporto tecnico limitato

- Esempi di servizi di raccolta (T3), che:
  - dispongono di un'installazione di prova
  - vengono sviluppati per un determinato cliente
  - possono non disporre di metadati o di documentazione
  - Supporto tecnico limitato

I servizi di raccolta consentono di accedere ai dati relativi agli eventi da varie origini ovvero:

- Sistemi di rilevamento delle intrusioni (host)
- Sistemi di rilevamento delle intrusioni (rete)
- Firewall
- Sistemi operativi
- Monitoraggio delle norme
- Autenticazione
- Router e switch
- VPN
- Antivirus
- Server Web
- Database
- Mainframe
- Valutazione delle vulnerabilità
- Servizi di directory
- Gestione di rete
- Sistemi proprietari

I servizi di raccolta sono costituiti da:

- File dei modelli
- File dei parametri
- File delle ricerche
- File di mappatura
- File di descrizione dei parametri e file manifest

Durante la creazione dello script del servizio di raccolta, il file dei modelli e il relativo file dei parametri vengono uniti in vari file di script.

A ogni file di script viene assegnato un nome in base al nome della colonna contenente la serie di valori del file dei parametri. I file di script vengono raggruppati in una sequenza ordinata all'interno delle sequenze di avvio e di backout.

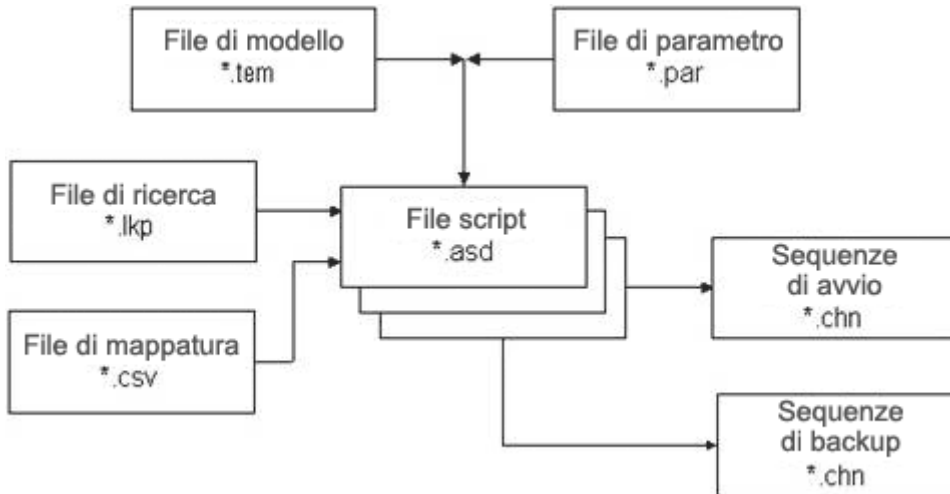
Queste ultime vengono assegnate a una porta, che esegue la serie di script al suo interno quando viene avviata o arrestata. Per essere utilizzato da una porta, gli script devono essere inclusi in una sequenza di avvio o di backout. Le porte consentono ai servizi di raccolta di individuare gli host Wizard all'interno della rete grazie all'indirizzo IP o al nome degli host in questione. Esse forniscono inoltre a Sentinel le informazioni relative alla posizione dei sensori e al servizio di raccolta utilizzato per gestire i dati provenienti da questi ultimi. È possibile configurare le opzioni seguenti per le porte:

- Tipo di connessione
  - Seriale: lettura dati da una porta seriale RS-232C
  - Socket: una connessione socket TCP
  - File nuovi: legge solo i dati degli eventi di sicurezza che vengono aggiunti al file dopo l'avvio dello script (legge a partire dalla fine del file)
  - File tutti: legge tutti i dati degli eventi di sicurezza inclusi in un file
  - Processo persistente: avvia un processo persistente al momento dell'avvio della porta, comunica con il Servizio di raccolta assegnato alla porta e con un'applicazione esterna ricevendo e trasmettendo gli stati, continua a eseguire il processo per l'intero esercizio della porta.
  - Processo transitorio: comunica con il Servizio di raccolta assegnato alla porta e con un'applicazione esterna ricevendo e trasmettendo gli stati. I processi transitori possono venire avviati più volte.

- SNMP: riceve i trap SNMP v1, v2 e v3
- Nessuno

- Nome del servizio di raccolta: è possibile rinominare, copiare e aggiungere servizi di raccolta

Quando un modello utilizza il comando di analisi sintattica LOOKUP(), viene effettuata una ricerca nel file appropriato per individuare un determinato blocco di comandi di analisi da eseguire.

Quando un modello utilizza il comando di analisi sintattica TRANSLATE, viene caricato un file di mappatura che consente di cercare rapidamente le voci chiave.

File dei modelli

È possibile creare, modificare, eliminare e aggiungere stati ai modelli. I modelli determinano il modo in cui i record vengono elaborati. La maggior parte delle decisioni relative ai modelli dipendono dal tipo di record utilizzati e dal loro formato. È disponibile un file di modelli equivalente con estensione .tem, che si trova nella posizione $WORKBENCH_HOME/Elements/<nome servizio di raccolta>/Docs/

I file dei modelli si basano sugli stati. Uno stato è un punto di decisione all'interno del flusso o del percorso logico di un modello. Ogni punto (stato) contiene informazioni che indicano il processo da eseguire. Gli stati contengono riferimenti ai parametri e, quando il modello viene unito a un file di parametri, i valori specifici sostituiscono i parametri stessi. In questo caso, vengono creati uno o più file di script.

Quando uno stato viene inserito in un modello, gli viene assegnato un numero che rimarrà invariato, indipendentemente dalla posizione nella quale esso viene spostato all'interno del modello. Esistono tre raggruppamenti di stati:

- Gli stati Trasmissione, Ricezione, Decisione e Analisi sono numerati nell'ordine in cui vengono inseriti nel modello.
  - Stato di trasmissione (Tx): trasmette una stringa a una determinata porta
  - Stato Ricezione (Rx): definisce se Wizard riceve informazioni da un'applicazione per la sicurezza all'interno di un buffer. Le informazioni sono dedotte dalla definizione della porta.
  - Stato Decisione: utilizza una stringa di dati o una variabile per determinare a quale stato passare

- Stato Analisi: utilizza i comandi di analisi per creare modelli per l'elaborazione delle informazioni raccolte nel buffer di ricezione
- Gli stati Successivo e Vai a vengono identificati dal numero dello stato a cui fanno riferimento.
    - Stato Successivo: indica lo stato a cui passare nello script successivo
    - Stato Vai: utilizzato per tornare a uno stato differente all'interno dello script corrente
- Lo stato Arresto è sempre assegnato al numero zero. Indica quando interrompere l'elaborazione su una porta.

Stato Trasmissione

Lo stato Trasmissione invia una stringa o una variabile (in base al tipo di dati selezionato) al tipo di connessione configurato per il servizio di raccolta in questione. Se la connessione viene interrotta durante il passaggio allo stato di trasmissione e viene immesso un valore nella casella Rx/Tx Value (Valore Rx/Tx) nel pannello Port Information (Informazioni sulla porta), si verifica l'evento successivo e viene tentato di ripristinare la connessione.

Il ritardo tra i caratteri indica il numero di millisecondi (ms) che separano l'invio di ogni byte.

Stato Ricezione

Lo stato Ricezione specifica il metodo utilizzato da Wizard per determinare quando i dati vengono ricevuti dal servizio di raccolta. Nello stato Ricezione vengono specificati:

- Tipo di ricezione
- Byte minimi
- Stringhe di decisione per la delimitazione

Se la connessione viene interrotta durante il passaggio allo stato di trasmissione e viene immesso un valore nella casella Rx/Tx Value (Valore Rx/Tx) nel pannello Port Information (Informazioni sulla porta), si verifica l'evento successivo e viene tentato di ripristinare la connessione.

In base allo stato Ricezione del buffer di ricezione, vengono valorizzate automaticamente due variabili:

- s_RXBufferString contiene il testo ricevuto dal buffer di ricezione
- i_RXBufferLength contiene la lunghezza di s_RXBufferString

Questo equivale a eseguire il codice dello script seguente in base allo stato Ricezione:

- COPY(s_RXBufferString:)
- LENGTH(i_RXBufferLength,s_RXBufferString)

Le variabili valorizzate automaticamente consentono di effettuare facilmente confronti nello stato Decisione, quando si tratta di determinare se lo stato Ricezione abbia raggiunto il timeout (i_RXBufferLength = 0). Esse consentono inoltre di utilizzare direttamente il buffer di ricezione in tutta la variabile s_RXBufferString.

Tipi di ricezione: l'editor dei modelli consente di utilizzare quattro tipi di ricezione ovvero:

- Timeout: consente agli script di continuare l'elaborazione anche se non vengono ricevuti dati in un determinato intervallo di tempo. Se si seleziona "timeout", Wizard è in grado di ricevere dati fino al raggiungimento del timeout, definito dalla variabile RX_TIMEOUT_DELAY.
- Wait (Attesa): utilizzato principalmente quando si ricevono messaggi non richiesti relativi a eventi. Wizard attende la ricezione dei dati per l'intervallo "timeout".

NOTA: per i tipi di ricezione timeout e attesa, l'elaborazione all'interno dello script non procede fino a quando non viene ricevuto il numero minimo di byte o la durata dell'attesa raggiunge il valore di timeout.

- delim timeout (Delimitatore timeout): utilizza una stringa predefinita per indicare a Wizard che i dati sono stati ricevuti. I dati nella casella Delimiter Decide String (Stringa di decisione delimitazione) vengono confrontati con quelli registrati a mano a mano nel buffer di ricezione.
- delim wait (Delimitatore attesa): utilizzato quando si ricevono messaggi non richiesti. Una stringa di caratteri definita dall'utente indica a Wizard che i dati sono stati ricevuti. I dati nella casella Delimiter Decide String (Stringa di decisione delimitazione) vengono utilizzati per verificare i byte ricevuti a mano a mano. Quando si utilizza l'opzione delim wait (Delimitatore attesa), il parametro RX_TIMEOUT_DELAY è ininfluente.

NOTA: per i tipi di ricezione delim timeout (Delimitatore timeout) e delim wait (Delimitatore attesa), l'elaborazione all'interno dello script non procede fino a quando la il confronto con la stringa per la determinazione del delimitatore non restituisce il valore "true" e viene ricevuto il numero minimo di byte o la durata dell'attesa raggiunge il valore di timeout.

Byte minimi: il numero minimo di byte è il numero di byte che devono essere ricevuti prima che Wizard utilizzi il periodo di timeout di default oppure prosegua l'elaborazione. L'elaborazione nello script non continua fino a quando non viene ricevuto il numero minimo di byte.

Stringa di decisione per la delimitazione*:* viene completata quando il tipo di ricezione è delim timeout (Delimitatore timeout) o delim wait (Delimitatore attesa). L'elaborazione a livello del servizio di raccolta non passa allo stato successivo fino a quando la stringa di decisione per il delimitatore non corrisponde ai dati in ingresso e non è stato ricevuto il numero minimo di byte.

La stringa di decisione per la delimitazione è un'espressione regolare conforme a POSIX 1003.2.

Scenari per i tipi di ricezione: esistono quattro tipi di scenari per i tipi di ricezione ovvero:

- Scenario timeout: una volta raggiunto lo stato Ricezione, l'elaborazione si interrompe fino a quando non viene letto il numero minimo di byte o non trascorre il numero di secondi indicato da RX_TIMEOUT_DELAY. Una volta che Wizard ha ricevuto più del numero minimo di byte specificato, oppure il timeout è stato superato, l'elaborazione sulla porta del servizio di raccolta passa allo stato successivo previsto dallo script.
- Scenario Wait (Attesa): si attende che il servizio di raccolta di Wizard riceva il numero minimo di byte indicato nella casella Minimum Bytes (Byte minimi). Una volta che Wizard ha ricevuto più del numero minimo di byte specificato, l'elaborazione sulla porta del servizio di raccolta passa allo stato successivo previsto dallo script. In caso contrario, l'elaborazione sulla porta del servizio di raccolta non raggiunge mai il timeout.

- Scenario Delim Timeout (Delimitatore timeout): se viene rilevata la stringa di decisione per la delimitazione dopo avere ricevuto il numero minimo di byte indicato nell'apposita casella, i dati fino al delimitatore (compreso quest'ultimo) vengono memorizzati nel buffer di ricezione. In caso contrario, i dati non vengono trasferiti nel buffer di ricezione e l'elaborazione sulla porta del servizio di raccolta raggiunge il timeout nell'intervallo di default.
- Scenario Delim Wait (Delimitatore attesa): se viene rilevata la stringa di decisione per la delimitazione dopo avere ricevuto il numero minimo di byte indicato nell'apposita casella, l'elaborazione sulla porta del servizio di raccolta prosegue e i dati vengono elaborati. In caso contrario, i dati non vengono trasferiti nel buffer di ricezione e la porta non raggiunge il timeout. Qualora la stringa di decisione per la delimitazione non venga mai incontrata, l'elaborazione sulla porta servizio di raccolta non raggiunge mai il timeout. Se, invece, viene rilevata la stringa di decisione per la delimitazione, ma non è stato ricevuto il numero minimo di byte, l'elaborazione sulla porta del servizio di raccolta non raggiunge mai il timeout.

Stato Decisione

Lo stato Decisione valuta il contenuto del buffer o della variabile di ricezione per determinare l'azione da eseguire. Se le informazioni nel buffer di ricezione contengono il tipo di decisione selezionato, Gestione servizi di raccolta elabora il comando e restituisce il valore "true", quindi viene seguito il ramo Yes. In caso contrario, Gestione servizi di raccolta elabora il comando e restituisce il valore "false", quindi viene seguito il ramo No.

Il buffer di ricezione (ovvero le sue dimensioni) è un parametro modificabile che si trova nella posizione seguente:

```
$WORKBENCH_HOME/config/wizard.properties/
   system.max_receive_buffer_size
```

Il parametro consente di configurare il buffer di ricezione di Gestione servizi di raccolta. Il default è 50.000 eventi, mentre il minimo è 5000 eventi. Quando il buffer di ricezione raggiunge le dimensioni massime, i nuovi eventi vengono rilasciati a mano a mano che vengono ricevuti, poiché sono bloccati.

Esistono quattro tipi per la decisione ovvero:

- String: confronta una stringa di decisione definita dall'utente con il contenuto del buffer di ricezione. Il contenuto della stringa di decisione viene confrontato con quello del buffer di ricezione, o di una variabile, per determinare quale ramo dell'albero decisionale elaborare. La stringa di decisione è un'espressione regolare conforme a POSIX 1003.2. Le variabili possono essere costituite da stringhe, interi e numeri decimali a virgola mobile.
- True: forza la valutazione a true, affinché Gestione servizi di raccolta segua il ramo Yes.
- True: forza la valutazione a false, affinché Gestione servizi di raccolta segua il ramo No.
- Data: confronta una stringa di decisione definita dall'utente con un'altra stringa o con il valore di una variabile.

Stato Analisi

Lo stato Analisi viene utilizzato per sviluppare gli script da eseguire sulle porte. I comandi di analisi possono comprendere parametri uniti al modello durante la creazione degli script. Per definire i comandi di analisi sono disponibili un editor visuale e un editor di testo.

Lo stato Analisi viene utilizzato inoltre per inserire comandi di analisi nei modelli. Questi comandi possono comprendere parametri e, quando il modello viene unito a un file

di parametri durante la creazione degli script, i valori specifici sostituiscono i parametri stessi. L'unione di modelli e file di parametri può dare origine a più script da eseguire sulle porte.

File dei parametri

I parametri sono equivalenti alle variabili. I file dei parametri (file .par) sono tabelle utilizzate per definire i nomi delle variabili nei file di script da eseguire associati. Essi sono utilizzati quando il codice di analisi contiene riferimenti e sono memorizzati come stringhe. È necessario convertire i valori numerici in stringhe affinché sia possibile utilizzarli. Quando vengono immessi nuovi valori per i parametri, essi diventano effettivi dopo la creazione dello script e, durante questo processo, vengono uniti al file dei modelli.

I nomi dei file di script da eseguire sono visualizzati nella prima riga della tabella, mentre i nomi dei parametri o etichette sono riportati nella prima colonna. La seconda riga della tabella è utilizzata per definire le icone visualizzate nell'albero del servizio di raccolta. Le altre righe si riferiscono allo script in questione e definiscono le variabili o i valori dei parametri da utilizzare come parametri.

I file dei parametri contengono i valori seguenti:

- Tag META, informazioni e commenti: sono disponibili oltre 200 tag META, di cui 100 possono essere configurati dall'utente e gli altri sono riservati.
- Rule (Regola): i nomi dei file delle serie sono visualizzati nella riga di intestazione della tabella, mentre i parametri sono riportati nella prima colonna.
- Bitmap: la seconda riga della tabella definisce le bitmap utilizzate per il file in questione, visualizzate nell'elenco dei servizi di raccolta.

File di ricerca

I file di ricerca sono tabelle facoltative (file .lkp) rispetto alle quali vengono confrontati i valori ricevuti per determinare quali azioni intraprendere, se necessario, in risposta agli eventi di sicurezza. I file di ricerca contengono clausole match, utilizzate per confrontare le singole stringhe. Sulla base delle clausole match di un file di ricerca specifico e i dati ricevuti dai dispositivi di origine, il comando LOOKUP determina se la stringa di ricerca è presente o assente.

I comandi di analisi possono eventualmente essere associati alla stringa match. I comandi di analisi vengono eseguiti se si trova una corrispondenza.

File di mappatura

I file di mappatura sono file opzionali (.csv) che consentono di eseguire una ricerca rapida delle voci chiave. Il file .csv è il percorso relativo di una directory di script del Servizio di raccolta. Attualmente questi file non possono essere modificati all'interno di Generatore servizi di raccolta, bensì utilizzando Excel.

Un esempio di file di mappatura è:

~Mese~	~Numero~
Gen	1
Feb	2
Mar	3
Apr	4
Mag	5
Giu	6
Lug	7
Ago	8
Set	9
Ott	10
Nov	11
Dic	12

Le voci possono essere costituite da variabili degli script (stringhe, variabili o decimali in virgola mobile) utilizzate per indicare le variabili nelle quali memorizzare i dati. Nell''esempio riportato i mesi vengono tradotti (mappati) in numeri (ad esempio, gennaio corrisponde a 1).

File manifest

I file manifest differenziano i servizi di raccolta della versione 5.* da quelli precedenti. Questi file consentono la distribuzione dei servizi di raccolta dalla Console Sentinel nonché la gestione delle versioni dei servizi stessi. L'analisi dei servizi di raccolta è definita nel file agent.lkp. I casi su cui viene effettuata la ricerca sono:

- Setup: impostazione di variabili e parametri; effettuata una sola volta.
- Check_Setup: verifica delle variabili e dei parametri impostati, effettuata una sola volta.
- Initialize_Vars: fase iniziale di ogni ciclo, nella quale le variabili vengono inizializzate una volta per analisi.
- Parse: luogo dove viene eseguita l'analisi.

Ciò consente di inserire l'analisi di nuovi servizi di raccolta nei modelli esistenti nonché di sovrapporre nuove versioni dell'analisi del servizio di raccolta per aggiornare il codice. Di seguito viene riportato l'elenco dei file manifest e il relativo contenuto per la versione 5.0:

- agent.nfo
  - product,Snort
  - product.vendor,GNU
  - product.version,2.0
  - product.security.type,IDS
  - product.sensor.type,N
  - product.name,IDSx_GNUx_SNRT
  - file.version,1

Altri riferimenti di Sentinel

Sono disponibili i manuali seguenti con i CD di installazione di Sentinel.

- Guida all'installazione di Sentinel™
- Guida dell'utente di Sentinel™ 5
- Guida dell’utente di Sentinel™ Wizard
- Guida di riferimento dell'utente di Sentinel™
- Guida all'integrazione di soluzioni di terze parti di Sentinel™
- Note di rilascio

Come contattare Novell

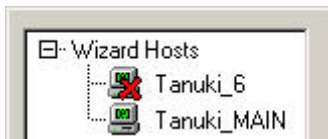
- Sito Web: http://www.novell.com
- Supporto tecnico Novell: http://www.novell.com/support/index.html
- Supporto tecnico Novell internazionale: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Supporto in autonomia: http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog
- Per supporto 24x7, 800-858-4000

2 Gestione di host Wizard

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Gli host Wizard sono computer sui quali è installata la funzione Gestione servizi di raccolta. Essi interagiscono con i computer che eseguono il Generatore servizi di raccolta e con Sentinel per mezzo della rete. I servizi di raccolta ricevono e analizzano i dati, in base ai quali gli host inviano avvisi a Sentinel.

Wizard rileva automaticamente gli host appartenenti alla rete e li aggiunge all'elenco contenuto nella scheda Host Wizard. Non è possibile aggiungere host manualmente, ma è possibile rinominare quelli esistenti ed eliminare quelli che non sono più fisicamente presenti e in grado di comunicare tramite la rete.

Il Generatore servizi di raccolta riceve tutti i messaggi relativi allo stato degli host e nell'albero degli host Wizard viene visualizzata una X rossa in corrispondenza degli host che non rispondono con un messaggio di stato. È possibile rimuovere gli host contrassegnati da una X rossa, ma se il Generatore servizi di raccolta rileva comunicazioni provenienti da questo host, esso viene nuovamente visualizzato nell'albero. Analogamente, se si rimuove un host in fase di comunicazione, il messaggio di stato fa in modo che esso venga reintegrato nell'albero degli host Wizard.

Agli host viene assegnato un numero identificativo non appena vengono rilevati.

I servizi di raccolta più recenti sono disponibili nel CD del Service Pack. Per ulteriori informazioni, vedere le Note di rilascio del Service Pack.

NOTA: per ulteriori informazioni relative alla configurazione dei servizi di raccolta dimostrativi, vedere il capitolo Test dell'installazione della Guida all'installazione di Sentinel.

Modalità di acquisizione dei dati sui servizi di raccolta da parte degli host Wizard

Per consentire agli host Wizard (computer in cui è installata la funzione Gestione servizi di raccolta) di ricevere dati da un servizio di raccolta, è necessario caricare il servizio in questione dal computer dove è installato il Generatore servizi di raccolta sull'host Wizard per mezzo di una porta configurata nel generatore stesso. Una volta caricato il servizio di raccolta nell'host, quest'ultimo è in grado di ricevere i dati dal servizio medesimo.

È possibile collegare ogni host Wizard a più porte affinché effettui il monitoraggio dei dati provenienti da più servizi di raccolta. Gli host Wizard possono disporre di porte per servizi

di raccolta che si collegano a vari tipi di origini dati. Per eseguire singoli servizi di raccolta su un porta host Wizard, è necessario caricarli. Le porte inoltre forniscono al Gestore dei servizi di raccolta informazioni sull'ubicazione delle origini dati.

Autorizzazioni degli host Wizard

Le autorizzazioni degli host Wizard vengono gestite per mezzo della scheda Amministratore di Sentinel Control Center. Le autorizzazioni utente relative agli host Wizard sono:

Autorizzazione	Descrizione
Visualizzazione dei servizi di raccolta	▪ Consente di visualizzare la scheda "Servizi di raccolta" in Sentinel Control Center ▪ Consente di visualizzare la scheda "Host Wizard" nel Generatore servizi di raccolta
Controllo dei servizi di raccolta	▪ Include tutte le funzionalità dell'autorizzazione relativa alla visualizzazione dei servizi di raccolta ▪ Consente il comando e il controllo dei servizi di raccolta da Sentinel Control Center ▪ Consente il comando e il controllo dei servizi di raccolta da Generatore servizi di raccolta di Wizard
Amministrazione dei servizi di raccolta	▪ Include tutte le funzionalità dell'autorizzazione relativa ai comandi del servizio di raccolta ▪ Nel Generatore servizi di raccolta, modifica e distribuzione del servizio di raccolta ▪ Nel Generatore servizi di raccolta, creazione, modifica, compilazione e debug dei servizi di raccolta ▪ Nel Generatore servizi di raccolta, caricamento e download dei servizi di raccolta ▪ Nel Generatore servizi di raccolta, esportazione di Host Wizard ▪ Nel Generatore servizi di raccolta, aggiunta, modifica ed eliminazione di porte ▪ Nel Generatore servizi di raccolta, impostazione delle opzioni Porta

Comando e controllo includono:

- avvio/interruzione di singole porte
- avvio/interruzione di tutte le porte
- riavvio di host
- ridenominazione di host

Gestione di host Wizard

In questo capitolo vengono trattati gli argomenti seguenti:

Avvio e arresto di Gestione servizi di raccolta

NOTA: quando si esegue Generatore servizi di raccolta di Wizard per la prima volta, può essere visualizzato un messaggio indicante che la directory 'Collectors' non esiste e verrà creata automaticamente. In questo caso alcune informazioni potrebbero essere perse. Scegliere OK. La directory verrà creata e Generatore servizi di raccolta di Wizard verrà avviato. Se questo messaggio viene visualizzato anche successivamente alla prima volta in cui viene eseguito Generatore servizi di raccolta di Wizard, è possibile che la directory Collectors sia stata eliminata inavvertitamente e sarà necessario verificare l'eventuale perdita di informazioni.

Avvio e arresto del servizio Gestione servizi di raccolta in Windows

Avvio e arresto dei servizi Gestione servizi di raccolta in Windows

1. Fare clic su Start > Impostazioni > Pannello di controllo.
2. Nel Pannello di controllo, fare doppio clic su Strumenti di amministrazione, quindi fare clic su Servizi.
3. Nella finestra di dialogo Servizi, fare clic con il pulsante destro del mouse su Gestione servizi di raccolta e fare clic su Avvia o Arresta.

Avvio dei servizi Gestione servizi di raccolta in Windows (riga di comando)

1. Aprire %WORKBENCH_HOME%
2. Per avviare Gestione servizi di raccolta:
   - ./agent-manager start
   - ./agent-manager restart: avvia in background lo script Gestione servizi di raccolta e, se è interrotto, avvia automaticamente il processo Gestione servizi di raccolta. Se il processo agentmanager è già in esecuzione, esso viene interrotto e riavviato.
   - ./agent-manager.sh console: avvia il processo Gestione servizi di raccolta in primo piano.

NOTA: nella modalità console, accertarsi di eseguire una sola istanza di Gestione servizi di raccolta nel computer.

Arresto dei servizi Gestione servizi di raccolta in Windows (riga di comando)

1. Aprire %WORKBENCH_HOME%
2. Per arrestare Gestione servizi di raccolta:

```
./agent-manager stop
```

Avvio di Gestione servizi di raccolta in UNIX (normale e console)

Avvio di Gestione servizi di raccolta in UNIX

1. In qualità di utente esecadm, passare alla directory:

```
$WORKBENCH_HOME
```

2. Immettere il comando seguente:

```
./agent-manager.sh start
```

- ./agent-manager.sh restart: avvia in background lo script Gestione servizi di raccolta e, se è interrotto, avvia automaticamente il processo Gestione servizi di raccolta. Se il processo Gestione servizi di raccolta è già in esecuzione, esso viene interrotto e riavviato.
- ./agent-manager.sh console: avvia il processo Gestione servizi di raccolta in primo piano.

Arresto di Gestione servizi di raccolta in UNIX

Arresto di Gestione servizi di raccolta in UNIX

1. In qualità di utente esecadm, passare alla directory:

```
$WORKBENCH_HOME
```

2. Immettere il comando seguente:

```
./agent-manager.sh stop
```

Amministrazione di Gestione servizi di raccolta

Sono disponibili un file eseguibile (Windows) e uno script (UNIX) di Gestione servizi di raccolta che consentono di:

- Installare il servizio Gestione servizi di raccolta (solo per Windows).
- Rimuovere il servizio Gestione servizi di raccolta (solo per Windows).
- Impostare il servizio Gestione servizi di raccolta.
- Stampare informazioni di debug complete.
- Visualizzare la versione della build.
- Visualizzare la guida.

Installazione del servizio Gestione servizi di raccolta (solo per Windows)

Installazione del servizio Gestione servizi di raccolta (solo per Windows)

1. Al prompt dei comandi, passare a %workbench_home%.
2. Immettere il comando seguente:

```
agent-manager.bat -install
```

3. Per avviare il servizio, eseguire una delle operazioni seguenti:
   - Al prompt dei comandi, digitare:

     ```
     net start "agent manager"
     ```

   - Fare clic su Start > Impostazioni > Pannello di controllo. Fare doppio clic su Servizi e scegliere Gestione servizi di raccolta. Avviare il servizio Gestione servizi di raccolta.

NOTA: se la finestra Servizi è già aperta, fare clic su Azione > Aggiorna e avviare il servizio Gestione servizi di raccolta.

Rimozione del servizio Gestione servizi di raccolta (solo per Windows)

Rimozione del servizio Gestione servizi di raccolta (solo per Windows)

1. Arrestare Gestione servizi di raccolta eseguendo una delle operazioni seguenti:
   - Al prompt dei comandi, digitare:

     ```
     net stop "agent manager"
     ```

   - Fare clic su Start > Impostazioni > Pannello di controllo. Fare doppio clic su Servizi e scegliere Gestione servizi di raccolta. Arrestare il servizio Gestione servizi di raccolta. Chiudere la finestra Servizi.
2. Al prompt dei comandi, passare a %workbench_home%.
3. Immettere il comando seguente:

   ```
   agent-manager.bat -remove
   ```

Modifica della password di Gestione servizi di raccolta in Windows

NOTA: per soddisfare le rigorose configurazioni di sicurezza necessarie per la certificazione dei criteri comuni, è consigliabile utilizzare una password complessa con le caratteristiche seguenti:

1. Scegliere password costituite da un minimo di 8 caratteri, di cui almeno uno MAIUSCOLO, uno minuscolo, uno speciale (!@#$%^&*()_+) e uno numerico (0-9).

2. Non è possibile includere nella password l'indirizzo di e-mail o una parte qualsiasi del nome completo.

3. La password non deve essere una parola "comune", ovvero una parola inclusa nel dizionario o di uso gergale.

4. È necessario che nella password non siano incluse parole di alcuna lingua poiché esistono numerosi programmi per la violazione delle password in grado di elaborare milioni di possibili combinazioni di parole in pochi secondi.

5. È consigliabile scegliere una password facile da ricordare e allo stesso tempo complessa. Ad esempio, Mfhq5!ao (Mio Figlio Ha Quasi 5 Anni Ormai) oppure VaNdq#3a (Vivo a Napoli Da Quasi 3 anni).

Modifica della password di Gestione servizi di raccolta in Windows

1. Al prompt dei comandi, passare a %workbench_home%.
2. Immettere il comando seguente:

ATTENZIONE: non viene richiesta alcuna conferma della password, né la password precedente.

```
agent-manager.bat –password <nuova password>
```

3. Affinché la password diventi effettiva, eseguire una delle operazioni seguenti:
   - Al prompt dei comandi, digitare:

     ```
     net stop "agent manager"
     net start "agent manager"
     ```

   - Nel Generatore servizi di raccolta, fare clic con il pulsante destro del mouse sul computer host interessato e scegliere di riavviare l'host.
   - Fare clic su Start > Impostazioni > Pannello di controllo. Fare doppio clic su Servizi e scegliere Gestione agenti. Arrestare e avviare il servizio Gestione agenti.

Modifica della password di Gestione servizi di raccolta in UNIX

NOTA: per soddisfare le rigorose configurazioni di sicurezza necessarie per la certificazione dei criteri comuni, è consigliabile utilizzare una password complessa con le caratteristiche seguenti:

1. Scegliere password costituite da un minimo di 8 caratteri, di cui almeno uno MAIUSCOLO, uno minuscolo, uno speciale (!@#$%^&*()_+) e uno numerico (0-9).

2. Non è possibile includere nella password l'indirizzo di e-mail o una parte qualsiasi del nome completo.

3. La password non deve essere una parola "comune", ovvero una parola inclusa nel dizionario o di uso gergale.

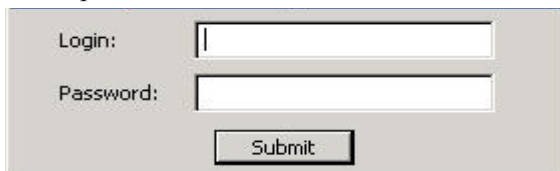
4. È necessario che nella password non siano incluse parole di alcuna lingua poiché esistono numerosi programmi per la violazione delle password in grado di elaborare milioni di possibili combinazioni di parole in pochi secondi.

5. È consigliabile scegliere una password facile da ricordare e allo stesso tempo complessa. Ad esempio, Mfhq5!ao (Mio Figlio Ha Quasi 5 Anni Ormai) oppure VaNdq#3a (Vivo a Napoli Da Quasi 3 anni).

Modifica della password di Gestione servizi di raccolta in UNIX

1. In qualità di utente esecadm, passare alla directory $WORKBENCH_HOME.
2. Immettere il comando seguente:

   ATTENZIONE: non viene richiesta alcuna conferma della password, né la password precedente.

   ```
   ./agent-manager.sh –password <nuova password>
   ```

3. Affinché la password diventi effettiva, passare alla directory /usr/local/bin e immettere il comando seguente:

   ```
   ./agent-manager.sh -restart
   ```

Avvio del Generatore servizi di raccolta

Avvio del Generatore servizi di raccolta

1. Fare clic su Start > Programmi > Sentinel > Generatore servizi di raccolta oppure fare doppio clic sull'icona Generatore servizi di raccolta sul desktop.
2. In base all'installazione in uso, eseguire il login come esecadm o mediante il nome utente per l'autenticazione in Windows.

Ridenominazione di host Wizard

Ridenominazione di host Wizard

1. In Generatore servizi di raccolta (Wizard), fare clic sulla scheda Host Wizard per aprire il pannello dell'albero corrispondente.
2. Nell'albero degli host Wizard, fare clic con il pulsante destro del mouse sull'host che si intende rinominare, quindi scegliere di ridenominare l'host. È possibile rinominare unicamente gli host attivi.
3. Immettere il nuovo nome dell'host e premere Invio.

NOTA: la ridenominazione non altera l'ID numerico assegnato agli host Wizard durante l'installazione. Questa informazione è memorizzata in %WORKBENCH_HOME%\wizard\agents\names.dat.

Eliminazione di host Wizard

Per eliminare un host è necessario prima rimuoverlo dalla rete, poiché non è possibile rimuovere host che comunicano attraverso di essa. Se un host è presente all'interno della rete ma non effettua alcuna comunicazione, nell'albero degli host Wizard la relativa icona è contrassegnata da una X rossa.

Eliminazione di host Wizard

1. Fare clic sulla scheda Host Wizard per visualizzare il pannello contenente l'albero omonimo.
2. Nell'albero Host Wizard, fare clic con il pulsante destro del mouse sull'host.
3. Fare clic su Elimina host.

Riavvio di host Wizard

Riavvio di host Wizard

1. Fare clic sulla scheda Host Wizard per visualizzare il pannello contenente l'albero omonimo e selezionare un host.
2. Fare clic con il pulsante destro del mouse su un host e scegliere di avviare le porte. È possibile riavviare unicamente gli host attivi.

Esportazione di host Wizard

Esportazione di host Wizard

1. Fare clic sulla scheda Host Wizard per visualizzare il pannello contenente l’albero omonimo. Selezionare un host.
2. Fare clic su File > Esporta host Verrŕ creata la sottodirectory seguente:

   ```
   %WORKBENCH_HOME%\upload_<nome host>
   ```

   È possibile spostare questa sottodirectory in un computer remoto per mezzo di Secure Shell (SSH) o utilizzando un disco. Una volta trasferita la sottodirectory nel computer remoto, eseguire il comando uploadhost. Questa operazione consente di copiare i file necessari nelle directory corrette.

NOTA: se le impostazioni SNMP vengono modificate, il Generatore servizi di raccolta non è in grado di comunicare con il computer remoto da quando viene premuto il pulsante Esporta a quando i file esportati del servizio di raccolta non vengono caricati.

Visualizzazione delle proprietà di host Wizard

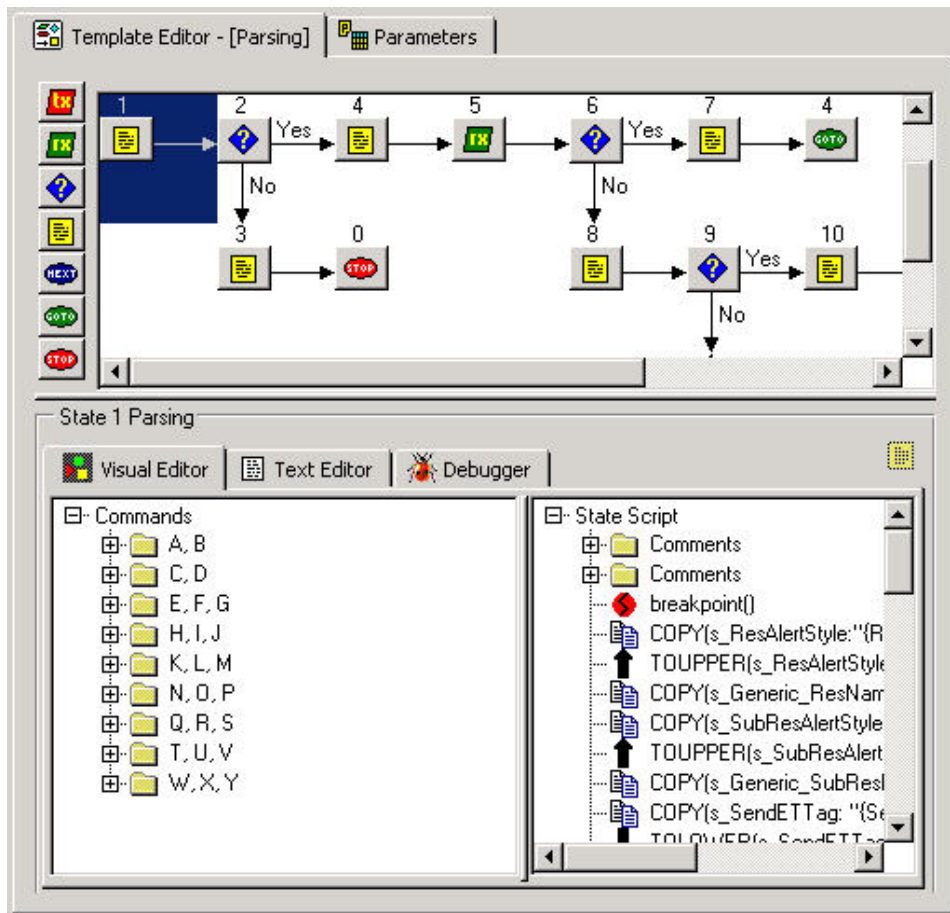
Visualizzazione delle proprietà di host Wizard

1. Fare clic sulla scheda Host Wizard per visualizzare il pannello contenente l’albero omonimo.
2. Nell’albero degli host Wizard, fare clic con il pulsante destro del mouse sull’host, quindi su Proprietŕ. Viene visualizzata la finestra Proprietŕ di Wizard, contenente le informazioni seguenti:
   - Nome
   - ID
   - Nome host
   - Indirizzo IP
   - Versione
   - Tempo di attività
3. Fare clic su OK per chiudere la finestra Proprietà.

NOTA: se l’host non è in funzione, scegliendo Proprietà viene visualizzata la finestra Nessuna risposta.

Modifica di file dei modelli

Modifica di file dei modelli

1. Fare clic sulla scheda Servizi di raccolta per visualizzare il pannello contenente l’albero omonimo.
2. Nell’albero Servizi di raccolta, fare clic sul modello, quindi sulla scheda dell'editor modelli sulla destra.
3. Nell’editor dei modelli, fare clic sullo stato che si intende variare e apportare le modifiche desiderate. Č possibile modificare gli stati utilizzando l’editor visuale o l’editor di testo. Per informazioni sui comandi di analisi, vedere la Guida di riferimento dell’utente di Sentinel.

Eliminazione di file dei modelli

Eliminazione di file dei modelli

1. Fare clic sulla scheda Servizi di raccolta per visualizzare il pannello contenente l'albero omonimo.
2. Nell'albero Servizi di raccolta, fare clic con il pulsante destro del mouse su un modello, quindi scegliere Elimina modello.

Ridenominazione di file di ricerca

Ridenominazione di file di ricerca

1. Fare clic sulla scheda Servizi di raccolta per visualizzare il pannello contenente l'albero omonimo.
2. Fare clic con il pulsante destro del mouse sul file di ricerca e scegliere di rinominare il file di ricerca.
3. Immettere il nuovo nome e premere Invio.

Eliminazione di file di ricerca

Eliminazione di file di ricerca

1. Fare clic sulla scheda Servizi di raccolta per visualizzare il pannello contenente l'albero omonimo.
2. Fare clic con il pulsante destro del mouse sul file di ricerca e scegliere di eliminare il file di ricerca.

Eliminazione di uno script

Eliminazione di uno script

1. Sono disponibili due metodi per eliminare uno script.
   - Nell'albero Servizi di raccolta, fare clic con il pulsante destro del mouse su uno script, quindi scegliere Elimina.
   - Fare clic con il pulsante destro del mouse sullo script nella colonna dello script di avvio e scegliere Elimina script.

Eliminazione di una sequenza di avvio

Eliminazione di una sequenza di avvio

1. Nel pannello dello script di avvio, scegliere la sequenza di avvio dal menu a discesa affinché il suo nome sia visualizzato nella casella dello script di avvio.
2. Fare clic con il pulsante destro del mouse sullo script interessato nell'albero dei servizi di raccolta e scegliere Elimina sequenza di avvio corrente. La sequenza di avvio viene rimossa dall'elenco degli script da eseguire all'avvio.

NOTA: se si elimina la sequenza di avvio di default, anche gli script assegnati a questa sequenza vengono eliminati dalla colonna dello script di avvio, ma quelli di default vengono comunque visualizzati nel menu Sequenze di avvio.

Porte Wizard

In questa sezione viene illustrato come arrestare, avviare, modificare, eliminare ed eseguire il debug delle porte Wizard.

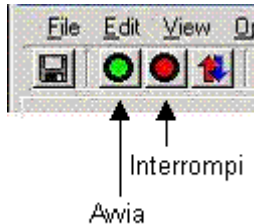
Avvio e arresto di porte Wizard – interfaccia utente grafica

Quando si avvia o si arresta un servizio di raccolta, i pulsanti corrispondenti nella colonna Avvia/Arresta cambiano quando il servizio di raccolta viene effettivamente avviato o arrestato. Se si interviene su un servizio di raccolta remoto, la modifica può essere differita in attesa della ricezione dello stato del servizio in questione.

L'avvio o l'arresto di una porta comporta l'esecuzione dello script di avvio e di backout selezionato.

Quando si avviano tutte le porte, ogni porta si avvia se la casella Esegui porta all'avvio di Altre opzioni porta del menu Opzioni è selezionata.

Avvio e arresto di tutte le porte Wizard

1. Nella finestra di Wizard:
   - Per arrestare tutte le porte, fare clic sul pulsante di arresto sulla barra degli strumenti.
   - Per avviare tutte le porte, fare clic sul pulsante di avvio sulla barra degli strumenti.

Avvio e arresto di una porta Wizard

1. Nella finestra di Wizard:
   - Per arrestare una porta, fare clic sul pulsante di arresto nella colonna Avvia/Arresta corrispondente alla porta in questione.
   - Per avviare una porta, fare clic sul pulsante di avvio nella colonna Avvia/Arresta corrispondente alla porta in questione.

Modifica di porte Wizard

Se si modifica la configurazione di una porta mentre essa è in funzione, la porta si arresta. Per evitare la perdita dei dati, arrestare la porta manualmente prima di modificarne la configurazione.

Modifica di porte Wizard

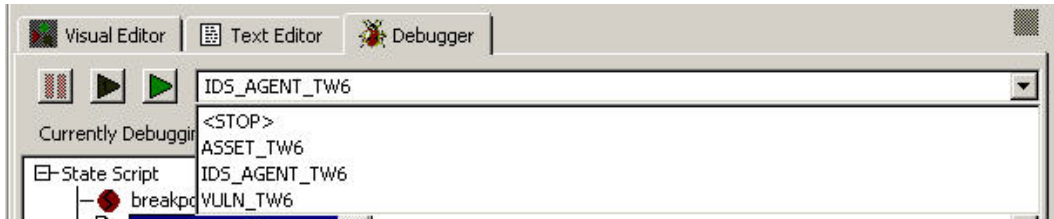
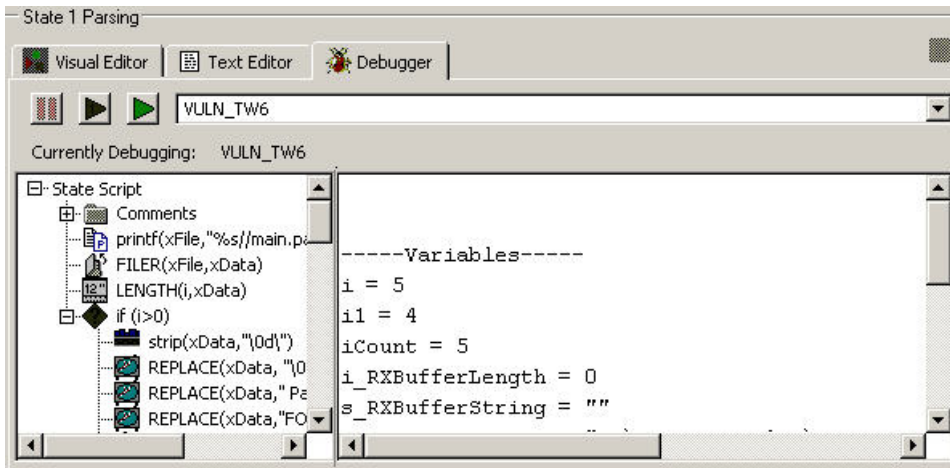
1. Dall'host interessato, arrestare la porta.
2. Seguire i passaggi per la creazione di una porta Wizard illustrati nel capitolo 3. La nuova configurazione sostituisce quella esistente quando si effettua il salvataggio o si carica la porta.

Eliminazione di porte Wizard

Eliminazione di porte Wizard

1. Arrestare la porta.
2. Nel pannello con le informazioni sulla porta del Generatore servizi di raccolta, fare clic con il pulsante destro del mouse e scegliere Elimina porta. Tutte le porte successive a quella eliminata vengono arrestate automaticamente.
3. Se l'eliminazione viene seguita da:
   - Host locale: fare clic su File > Salva e selezionare l'opzione Informazioni sulla porta.
   - Host remoto: fare clic su File > Carica/Scarica.

Debug delle porte Wizard

Il debugger consente di risolvere i problemi del codice del servizio di raccolta in esecuzione su una porta. Il lato sinistro del pannello Debugger mostra lo script di stato. Il lato destro del pannello mostra gli script e le variabili RX_Buffer, il cui nome può essere lungo fino a 32 caratteri.

Affinché il debugger sia efficace, è necessario che il primo stato sia uno stato di analisi e che vi siano comandi Breakpoint().

Durante il debug, attendere l’aggiornamento del buffer di ricezione prima di eseguire un’altra funzione.

NOTA: se l’host della Gestione servizi di raccolta ha perso la connettività ( ), non è possibile eseguire il debug delle relative porte.

Debug delle porte Wizard

1. Nell’editor dei modelli, scegliere la scheda Debugger nel pannello di modifica per accedere al Debugger. Viene visualizzato un pannello vuoto, che consente di selezionare da un elenco a discesa la porta Wizard della quale si intende eseguire il debug.

   Facendo clic sulla scheda Host Wizard, la porta in fase di debug indica che si trova in questa modalità.

VULN_TW6	File All	C:\workarea\vuln_inf	DemoVulnerabilityUploa	Stop	Debug
ASSET_TW6	File All	c:\workarea\asset_o	T1_GNUx_NMAP_0355	Start	Off

2. Nell’elenco a discesa, selezionare una porta per avviare la procedura di debug. Effettuare il debug della porta eseguendo una delle seguenti operazioni:

- Premere F6 per eseguire un comando alla volta oppure fare clic sul pulsante per l'esecuzione di un comando.

  Fare di nuovo clic sul pulsante o premere F6 per riprendere l'esecuzione dello script.
- Premere F7 per eseguire i comandi oppure fare clic sul pulsante per la ripresa dell'esecuzione dei comandi.

  Premere F5 per sospendere l'esecuzione oppure fare clic sul pulsante per la sospensione dell'esecuzione dei comandi.

  L'esecuzione verrà sospesa finché non si preme F7 oppure il pulsante per la ripresa dell'esecuzione dei comandi.

Il debugger si ferma in corrispondenza di tutti i breakpoint, ma non interrompe l’esecuzione e lo stato delle porte è “attivo”.

Nella modalità debug, durante le pause non viene inviato alcun evento.

Al termine dell’analizzatore sintattico, i pulsanti diventano grigi e viene visualizzato il messaggio Nessuna porta in fase di debug.

Il debugger non interrompe le pause; per questo motivo, se si effettua il debug di un analizzatore che ha incontrato un comando di pausa, il pulsante Arresta o Passaggio attendono che la pausa termini prima di diventare effettivi.

Caricamento e download dei servizi di raccolta e degli host

La finestra Carica/Scarica contiene tre schede, ovvero:

- Host: carica la configurazione di ogni porta e la serie di servizi di raccolta in ognuno degli host specificati. Ogni host presenta ancora la propria configurazione delle porte e la propria serie di servizi di raccolta.
- Servizi di raccolta: per il caricamento di singoli servizi di raccolta.
- Popola rete: carica la configurazione delle porte e/o gli agenti di un determinato host in tutti gli host selezionati, che ricevono la stessa configurazione delle porte e la stessa serie di servizi di raccolta dell’host di origine.

Durante il download, la configurazione delle porte di un servizio di raccolta remoto viene visualizzata sull’host di cui si sta effettuando il download e tutti i servizi di raccolta dell’host remoto aventi lo stesso nome di quelli dell’host locale vengono sovrascritti.

Caricamento di un servizio di raccolta in un solo host

Caricamento di un servizio di raccolta in un solo host

1. Se il servizio di raccolta è già configurato correttamente e lo script è stato creato, è possibile ignorare i passaggi da 2 a 11.
2. Fare clic sulla scheda Host Wizard e scegliere un host.
3. Nella colonna Nome porta, fare clic su Nuovo e immettere il nome desiderato.
4. Scegliere un servizio di raccolta nella colonna omonima.
5. Configurare il servizio di raccolta come indicato dalla documentazione (%WORKBENCH_HOME%\Elements\<nome servizio di raccolta>\docs\<nome file>.pdf).

6. Fare clic sulla scheda Servizi di raccolta, espandere il servizio in questione ed evidenziare il file del modello.
7. Sul lato destro, fare clic sulla scheda dei parametri.
8. Impostare i valori dei parametri desiderati, come descritto nella documentazione del servizio di raccolta.
9. (operazione facoltativa) Se si desidera che il servizio di raccolta non venga avviato all'avvio o che consideri valido l'orario del dispositivo, fare clic sulla scheda Host Wizard, fare clic con il pulsante destro del mouse sul nome della porta Wizard, scegliere Altre opzioni porta e deselezionare la voce Esegui porta all'avvio o selezionare la voce Considera valida l'ora del dispositivo. Fare clic su OK.

10. Fare clic su Salva.
11. Fare clic sulla scheda Servizi di raccolta, fare clic con il pulsante destro del mouse sul file dei modelli e scegliere Genera script.
12. Fare clic su una delle opzioni seguenti:
    - *File > Carica/Scarica.*
    - Fare clic con il pulsante destro del mouse sul servizio di raccolta, quindi scegliere Carica servizio di raccolta.
    - Pulsante Carica/Scarica .

    Viene visualizzata la finestra Carica/Scarica.
13. Nella finestra Carica/Scarica, fare clic sulla scheda Servizi di raccolta.
14. Nell'elenco a discesa, selezionare il servizio di raccolta che si desidera caricare.
15. Fare clic su Carica. La prima volta che si esegue questa operazione, viene chiesta la password di Gestione servizi di raccolta, anche nel caso di host Wizard locali. Verrà visualizzata la finestra di avanzamento trasferimento relativa al caricamento.

NOTA: è possibile utilizzare la finestra di avanzamento per riavviare gli host dopo un trasferimento.

Caricamento di un servizio di raccolta in più host

Caricamento di un servizio di raccolta in più host

ATTENZIONE: se si effettua il caricamento di un host che presenta un servizio di raccolta con lo stesso nome di uno all'interno dell'host locale, il servizio di raccolta dell'host remoto viene sovrascritto senza alcun preavviso.

1. Se il servizio di raccolta è già configurato correttamente e lo script è stato creato, è possibile ignorare i passaggi da 2 a 11.
2. Fare clic sulla scheda Host Wizard e scegliere un host.
3. Nella colonna Nome porta, fare clic su Nuovo e immettere il nome desiderato.

4. Scegliere un servizio di raccolta nella colonna omonima.
5. Configurare il servizio di raccolta come indicato dalla documentazione (%WORKBENCH_HOME%\Elements\<nome servizio di raccolta>\docs\<nome file>.pdf).
6. Fare clic sulla scheda Servizi di raccolta, espandere il servizio in questione ed evidenziare il file del modello.
7. Sul lato destro, fare clic sulla scheda dei parametri.
8. Impostare i valori dei parametri desiderati, come descritto nella documentazione del servizio di raccolta.
9. (operazione facoltativa) Se si desidera che il servizio di raccolta non venga avviato all'avvio o che consideri valido l'orario del dispositivo, fare clic sulla scheda Host Wizard, fare clic con il pulsante destro del mouse sul nome della porta Wizard, scegliere Altre opzioni porta e deselezionare la voce Esegui porta all'avvio o selezionare la voce Considera valida l'ora del dispositivo. Fare clic su OK.
10. Fare clic su Salva.
11. Fare clic sulla scheda Servizi di raccolta per visualizzare il pannello contenente l'albero omonimo.
12. Fare clic su un servizio di raccolta.
13. Fare clic su una delle opzioni seguenti:
    - File > Carica/Scarica.
    - Fare clic con il pulsante destro del mouse sul servizio di raccolta, quindi scegliere Carica servizio di raccolta.
    - Pulsante Carica/Scarica .

    Viene visualizzata la finestra Carica/Scarica.
14. Nella finestra Carica/Scarica, fare clic sulla scheda Host e selezionare o deselezionare la casella di controllo Carica i servizi di raccolta durante il caricamento.

    Se questa casella di controllo è selezionata, i servizi di raccolta selezionati nella scheda omonima vengono caricati. Questa casella di controllo è selezionata di default. Quando si effettua il download di un servizio di raccolta da un host, essa non ha alcun effetto.
15. Nell'elenco, selezionare gli host Wizard nei quali si desidera caricare i servizi di raccolta.

    Tutti gli host Wizard della rete vengono inclusi automaticamente nell'elenco. I pulsanti indicano se il computer host è in linea.

    Fare clic su Seleziona tutto per selezionare tutti gli host Wizard dell'elenco. Fare clic su Nessuna selezione per deselezionare tutti gli host Wizard dell'elenco.
16. Fare clic su Carica per caricare i servizi di raccolta selezionati negli host desiderati. La prima volta che si esegue questa operazione, viene chiesta la password di Gestione servizi di raccolta, anche nel caso di host Wizard locali.

Download di un host

Download di un host

ATTENZIONE: se si scarica un host che presenta un servizio di raccolta con lo stesso nome di uno all'interno dell'host locale, il servizio di raccolta dell'host locale viene sovrascritto senza alcun preavviso.

1. Fare clic sulla scheda Host Wizard per visualizzare il pannello contenente l'albero degli host.
2. Nell'albero degli host Wizard, fare clic sull'host del quale si desidera effettuare il download.
3. Fare clic su una delle opzioni seguenti:
   - File > Carica/Scarica.
   - Fare clic con il pulsante destro del mouse sul servizio di raccolta, quindi scegliere Carica servizio di raccolta.
   - Pulsante Carica/Scarica .

   Viene visualizzata la finestra Carica/Scarica. Il servizio di raccolta selezionato è contrassegnato di default.
4. Fare clic su Scarica. La prima volta che si esegue questa operazione, viene chiesta la password di Gestione servizi di raccolta, anche nel caso di host Wizard locali. Viene effettuato il download dell'host, che viene aggiunto all'albero degli host Wizard. Viene visualizzata la finestra di avanzamento trasferimento relativa al download.

   NOTA: è possibile utilizzare la finestra di avanzamento per riavviare gli host dopo un trasferimento.

   NOTA: è possibile effettuare il download di un solo host per volta. Se si selezionano più host, il download non viene eseguito.

Download dei servizi di raccolta da un host

Download dei servizi di raccolta da un host

1. Fare clic su una delle opzioni seguenti:
   - File > Carica/Scarica.
   - Pulsante Carica/Scarica .

   Viene visualizzata la finestra Carica/Scarica.
2. Nell'elenco, selezionare l'host Wizard da cui si desidera effettuare il download dei servizi di raccolta.

   Tutti gli host Wizard della rete vengono inclusi automaticamente nell'elenco. I pulsanti indicano se il computer host è in linea.

   Fare clic su Seleziona tutto per selezionare tutti gli host Wizard dell'elenco. Fare clic su Nessuna selezione per deselezionare tutti gli host Wizard dell'elenco.
3. Fare clic su Scarica per caricare i servizi di raccolta dagli host selezionati.

Caricamento di porte in più host

Caricamento di porte in più host

1. Fare clic su una delle opzioni seguenti:
   - File > Carica/Scarica.
   - Pulsante Carica/Scarica .
2. Viene visualizzata la finestra Carica/Scarica.

3. Nella finestra Carica/Scarica, fare clic sulla scheda Popola rete.
4. Nell’elenco denominato Configurazioni delle porte host e dei servizi di raccolta che si desidera caricare, scegliere l’host in cui desidera caricare le impostazioni per la configurazione delle porte e i servizi di raccolta.
5. Nell’elenco denominato Host nei quali si desidera caricare questa configurazione, scegliere l’host in cui desidera caricare le impostazioni selezionate.

   Tutti gli host Wizard della rete vengono inclusi automaticamente nell’elenco. I pulsanti indicano se il computer host è in linea.

   Fare clic su Seleziona tutto per selezionare tutti gli host Wizard dell’elenco. Fare clic su Nessuna selezione per deselezionare tutti gli host Wizard dell’elenco.

Caricamento di più servizi di raccolta in una rete

Caricamento di più servizi di raccolta in una rete

1. Nella finestra principale di Wizard scegliere un servizio di raccolta nell’albero omonimo.
2. Fare clic su una delle opzioni seguenti:
   - File > Carica/Scarica.
   - Fare clic con il pulsante destro del mouse sul servizio di raccolta, quindi scegliere Carica servizio di raccolta.
   - Pulsante Carica/Scarica .
3. Selezionare la scheda Popola rete.
4. Nel primo riquadro di selezione, nel menu a discesa, selezionare la configurazione delle porte e i servizi di raccolta dell'host che si desidera caricare.
5. Nel secondo riquadro di selezione, nel menu a discesa, selezionare gli host nei quali si desidera effettuare il caricamento della configurazione.

   NOTA: per caricare la configurazione, è necessario effettuare almeno una selezione in almeno uno dei due riquadri.

   È possibile selezionare un servizio di raccolta diverso in ciascun riquadro. Ogni servizio di raccolta selezionato nell’elenco principale acquisisce la configurazione delle porte e i servizi di raccolta dell’host selezionato nel riquadro con l’etichetta:

   Configurazioni delle porte host e dei servizi di raccolta che si desidera caricare, a meno che non sia stata selezionata l’opzione Nessuno.

6. Una volta completata l’impostazione della configurazione di rete, scegliere il pulsante Carica per iniziare il caricamento.

Upgrade dei servizi di raccolta

Upgrade dei servizi di raccolta

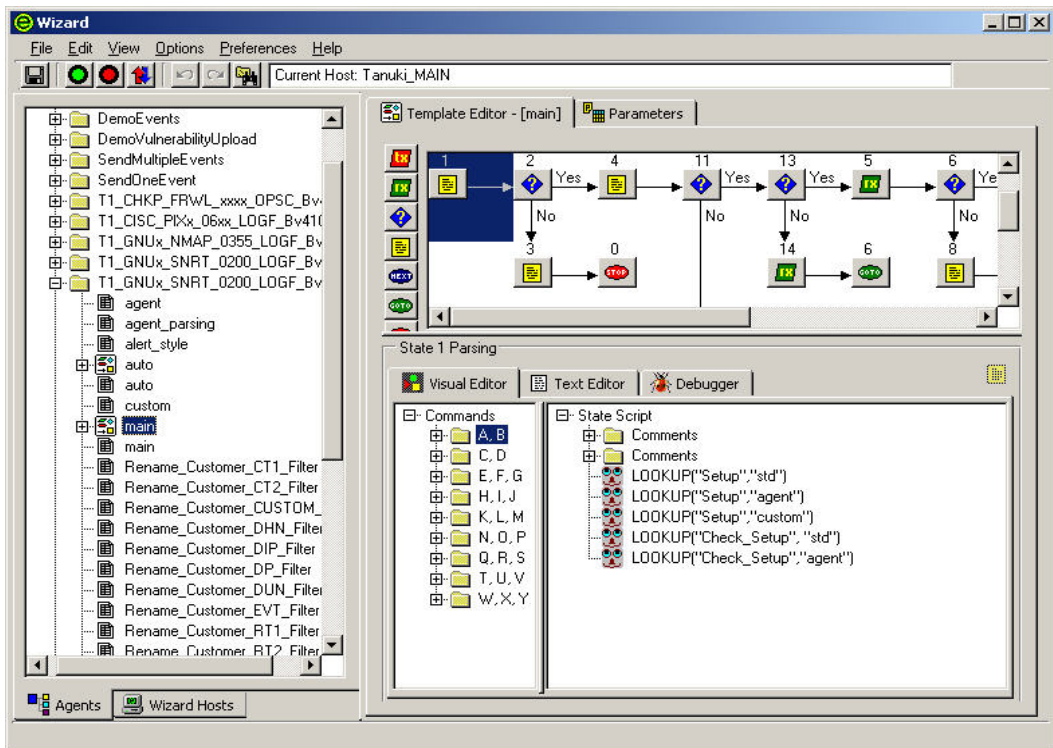
1. Leggere la documentazione fornita con il nuovo servizio di raccolta, che descrive le eventuali modifiche.
2. Memorizzare la nuova versione del servizio di raccolta nella directory %workbench_home%/Elements del computer principale per il servizio di raccolta in questione.
3. Aprire il file dei parametri del servizio di raccolta che si sta sostituendo e tagliare e incollare i parametri uguali nel nuovo servizio.

4. Se necessario, come indicato nella documentazione del nuovo servizio di raccolta, eliminare o aggiungere nuove variabili ai parametri. Se si aggiungono nuove variabili, č necessario popolarle.
5. Salvare il file dei parametri nel nuovo servizio di raccolta.
6. Creare il nuovo servizio di raccolta.
7. Modificare le informazioni relative alla configurazione della porta per utilizzare il nuovo servizio di raccolta.
8. Salvare le informazioni relative alla configurazione della porta.
9. Caricare il nuovo servizio di raccolta e la configurazione della porta.
10. Riavviare la porta.

3 Generazione e manutenzione dei servizi di raccolta

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

NOTA: Per gli utenti di MS SQL 2000, la dimensione degli eventi non può superare gli 8 KB.

I servizi di raccolta analizzano i dati provenienti da un’origine di eventi di sicurezza e li inviano a Sentinel. Essi vengono creati, attivati e mantenuti mediante la procedura guidata Generatore servizi di raccolta Fare clic sulla scheda Servizi di raccolta per visualizzare l’albero corrispondente e individuare tutti i servizi di raccolta e i relativi componenti disponibili nel sistema Sentinel in uso.

Gestione servizi di raccolta consente di:

- Generare servizi di raccolta
  - Creare e configurare i file dei modelli
  - Creare i file dei parametri
  - Creare i file di ricerca
  - Generare script
  - Creare una porta di Wizard

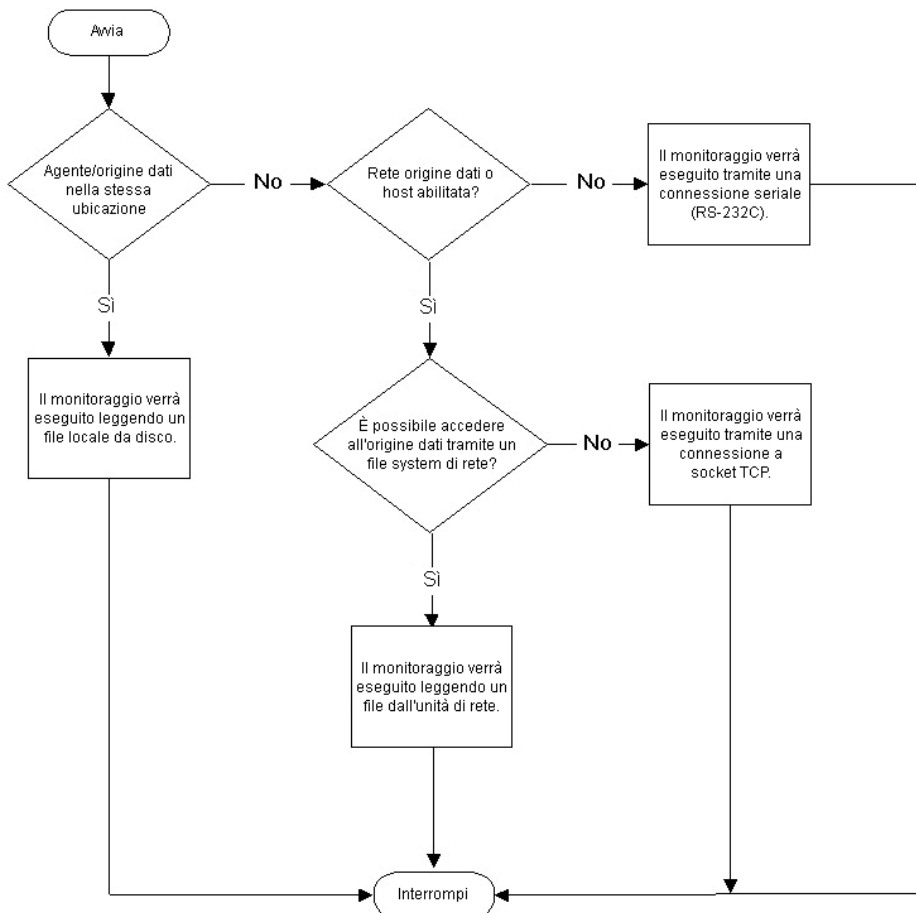
Cenni sulla generazione di servizi di raccolta

I passaggi fondamentali per la generazione di servizi di raccolta sono:

- Creazione e configurazione del file dei modelli, compresi i punti di decisione basati sulle modalitŕ di applicazione degli stati.
- Creazione e configurazione del file dei parametri
- Creazione e configurazione del file di ricerca (facoltativo)
- Generazione dello script
- Assegnazione di una sequenza di avvio
- Creazione della porta, assegnazione del servizio di raccolta alla porta e suo avvio

Passaggi fondamentali per l'implementazione dei servizi di raccolta

I passaggi fondamentali per implementare un servizio di raccolta sono i seguenti:

- Determinare ciò che si desidera monitorare
- Determinare come monitorare i dati
- Determinare il sistema operativo del prodotto
  - Se l'host e il prodotto sono co-locati, il modo più logico per acquisire i dati è leggerli nel file di log del prodotto.
  - Se, invece, l'host e il prodotto non si trovano nello stesso computer, è possibile ottenere i dati necessari mediante l'impostazione di un file system di rete (ad esempio, NFS, Samba o share SMB), una connessione socket TCP/IP oppure una connessione seriale.
- Generare i servizi di raccolta e avviare le porte.
- Se si utilizzano host remoti, caricare al loro interno i file dei servizi di raccolta. Avviare le porte per eseguire gli script di avvio: le informazioni raccolte vengono riportate attraverso il sistema Sentinel.

Generazione dei servizi di raccolta

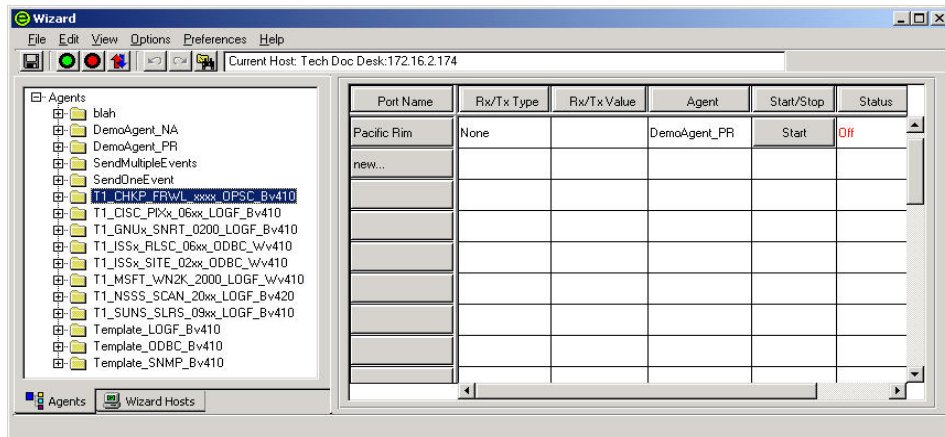
Come illustrato in precedenza, per generare un servizio di raccolta sono necessari:

- File dei modelli
- File dei parametri
- File di ricerca (facoltativo)
- Script
- Assegnazione del nome di una porta Wizard al servizio di raccolta

Creazione e configurazione dei file dei modelli

Creazione e configurazione dei file dei modelli

1. Avviare il Generatore servizi di raccolta.
2. Fare clic sulla scheda Servizi di raccolta per visualizzare il pannello contenente l'albero omonimo.
3. Nell'albero dei servizi di raccolta, fare clic con il pulsante destro del mouse su Servizi di raccolta, quindi fare clic su Nuovo servizio di raccolta.
4. Immettere il nome del nuovo servizio di raccolta nell'apposito spazio e premere Invio.

5. Fare clic con il pulsante destro del mouse sul nuovo servizio di raccolta, quindi fare clic su Nuovo modello.

6. Nella casella Nuovo modello dell’albero dei servizi di raccolta, digitare il nome del modello e premere Invio.
7. Selezionare il nuovo modello e fare clic sulla scheda dell'editor di modelli.
8. Nel pannello dell'editor di modelli, trascinare e rilasciare gli stati nell’area di modifica mediante i pulsanti di stato a sinistra del pannello stesso.
   Per informazioni sull’aggiunta di stati a un modello, vedere la sezione Aggiunta di stati ai modelli.
9. Fare clic su Salva.

Aggiunta di stati ai file dei modelli

Tutti i servizi di raccolta iniziano l’elaborazione in corrispondenza dello stato 1, indipendentemente dalla posizione di quest’ultimo nel modello. Presumendo che lo stato 1 si riferisca a un’elaborazione, inserire il nuovo stato dopo lo stato 1.

Il Generatore servizi di raccolta assegna automaticamente il numero 1 al primo stato, pertanto è consigliabile che quest’ultimo contenga esclusivamente il comando di analisi BREAKPOINT(). L’inserimento di un solo breakpoint dopo lo stato 1 facilita il debug, poiché l’analizzatore sintattico si ferma automaticamente allo stato successivo.

Durante la creazione dei modelli, è opportuno iniziare con uno stato di analisi di tipo “solo breakpoint” e aggiungere lo stato operativo (Ricezione, Analisi e così via) nello stato 2. Qualora sia necessario aggiungere uno stato all’inizio del modulo, è preferibile eseguire questa operazione unicamente dopo il comando BREAKPOINT.

Non eliminare lo stato di analisi BREAKPOINT a meno che non sia necessario aggiungere un altro stato all’inizio del modello. È possibile inserire eventuali commenti nel comando BREAKPOINT per descrivere la funzionalità del modello.

Aggiunta di stati a un modello

1. Fare clic sulla scheda Servizi di raccolta per visualizzare il pannello contenente l’albero omonimo.
2. Nell’albero dei servizi di raccolta, scegliere un modello per visualizzare l’editor di modelli nel pannello destro.
3. Fare clic su Opzioni > Aggiungi stato > Trasmissione, Ricezione, Decisione, Analisi, Successivo, Vai a o Arresto, oppure fare clic sul pulsante corrispondente.

- Trasmissione
- Ricezione
- Decisione
- Analisi
- Successivo
- Vai a
- Interruzione

4. Mediante i pannelli di modifica nella parte inferiore del pannello dell'editor di modelli), inserire il nuovo codice in ogni stato a mano a mano che viene aggiunto.

   In alternativa è possibile trascinare e rilasciare un pulsante relativo allo stato Analisi dal lato sinistro dell'editor di modelli all'area di modifica.

NOTA: non utilizzare le virgolette doppie all'interno della stringa di decisione nello stato omonimo (ad esempio, per individuare il delimitatore in un file di log) o di decisione; in caso contrario, viene generato il messaggio di errore seguente:

```
***ERRORE: Lettura file del modello in corso..."
```

Qualora una o più virgolette siano inserire nella stringa di decisione o di delimitazione, viene generato l'errore seguente:

```
StateDecideString: "test"123"
```

La soluzione alternativa consiste nell'utilizzare \22\ invece delle virgolette (").

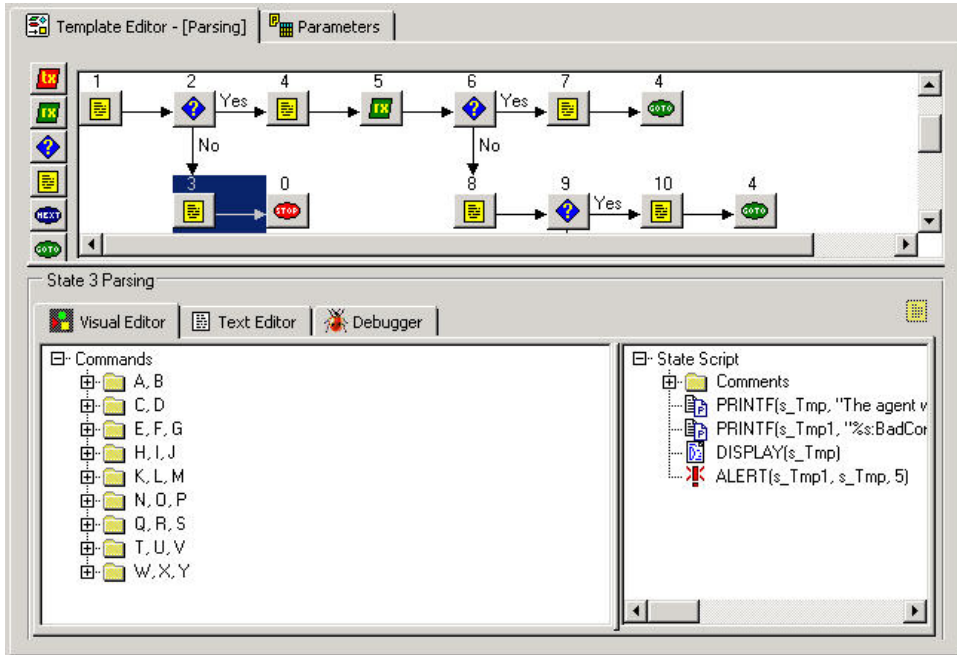
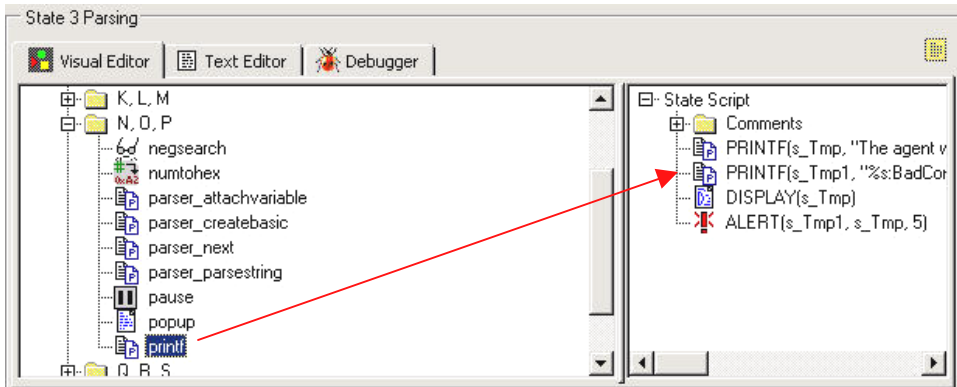
NOTA: se viene selezionato un altro elemento della scheda Servizi di raccolta (anche appartenente allo stesso servizio) e, quindi, si torna al modello errato, il Generatore servizi di raccolta visualizza il messaggio di errore seguente e non visualizza alcuna parte o stato del modello. L'errore si verifica perché le virgolette (“) vengono utilizzate per delimitare i valori dei campi in un file .tem. Ad esempio:

```
StateDecideString: "test"
StateDelimiterString: "123"
```

Immissione di comandi di analisi mediante l'editor visuale

Sono disponibili due metodi per l'immissione di un comando di analisi, l'editor visuale e l'editor di testo. È consigliabile limitare i comandi a 4096.

Immissione di comandi di analisi mediante l'editor visuale

1. Nell'editor di modelli, scegliere uno stato di analisi. Quando si fa clic su un modello per aprirlo, per default viene visualizzata la scheda dell'editor visivo.

2. Nell'editor visuale, trascinare i comandi di analisi verso il lato destro del pannello.

3. Immettere i valori degli argomenti nella finestra dell'editor dei comandi popup.
   - Scegliere un tipo: i tipi corrispondenti a ogni comando di analisi sono descritti nella Guida di riferimento dell'utente di Sentinel.
   - Specificare un valore: i valori vengono definiti per una determinata applicazione. Esempi di valori per ogni comando di analisi sono disponibili nella Guida di riferimento dell'utente di Sentinel.

Immissione di comandi di analisi mediante l'editor di testo

1. Nell'editor dei modelli, fare clic sulla scheda dell'editor di testo).
2. Immettere manualmente i comandi di analisi desiderati.

   Utilizzare il tasto Tab della tastiera per allineare il testo quando si utilizza un font fisso. È possibile copiare, tagliare e incollare le funzioni come in un normale editor di testo.

Modifica dei comandi di analisi

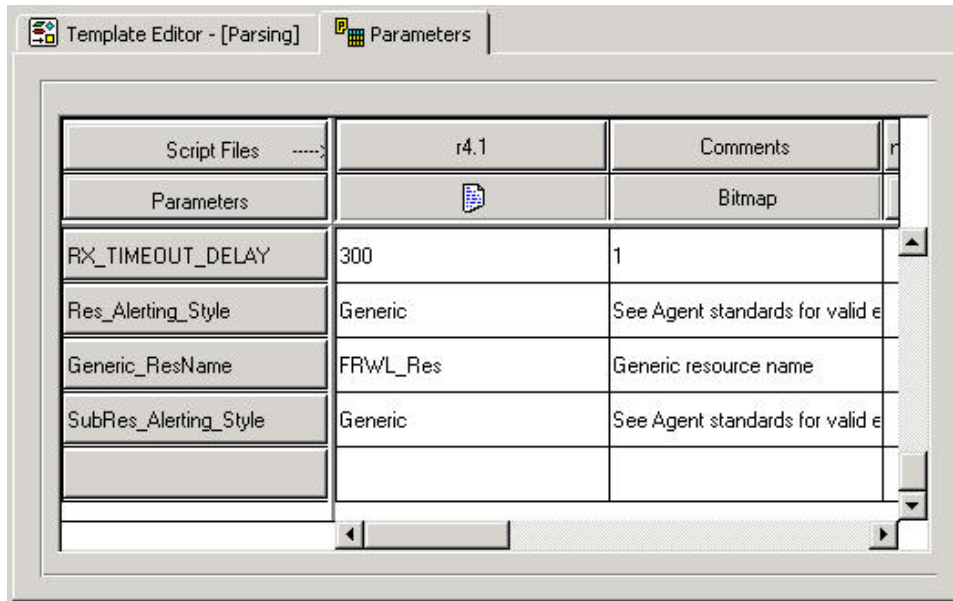
- Argomenti: contiene tutti gli argomenti possibili per il comando di analisi selezionato nell'editor visuale.
- Argument Use (Uso argomenti): definisce se l'argomento è obbligatorio o facoltativo.
- Tipo: determina il tipo di variabili, ad esempio stringhe, variabili stringa, numeri, numeri variabili, decimali a virgola mobile, variabili decimali a virgola mobile o variabili predefinite.
- Valore: indica il valore definito dall'utente per la variabile mostrata nella colonna Tipo.

Modifica dei comandi di analisi

1. Nell'editor visuale è possibile:
   - Fare clic con il pulsante destro del mouse su un comando di analisi e scegliere Aggiungi all'elenco analisi degli stati.
   - Fare doppio clic su un comando di analisi per aprire l'editor dei comandi.
2. Compilare le caselle Tipo e Valore per terminare la modifica. Per ulteriori informazioni sulla descrizione dei comandi di analisi, vedere la Guida di riferimento dell'utente di Sentinel.

Creazione e configurazione dei file dei parametri

Creazione e configurazione dei file dei parametri

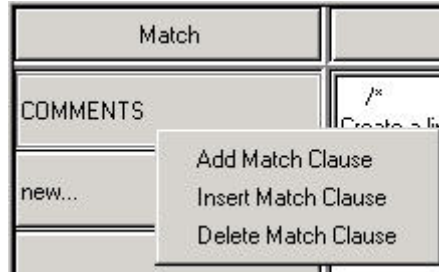
1. Fare clic sulla scheda Servizi di raccolta.
2. Scegliere un modello e pare clic sulla scheda Parametri nel pannello destro.

3. Fare doppio clic sul pulsante Nuovo nella prima colonna della tabella dei parametri.
4. Immettere il nome del nuovo parametro (si tratta del nome dello script, ad esempio r4.1) e premere Invio.
5. (Operazione facoltativa) Fare clic con il pulsante destro del mouse sul pulsante Bitmap (seconda colonna/seconda riga), quindi scegliere Assegna bitmap. Nella finestra di dialogo per l'assegnazione bitmap, scegliere un pulsante Bitmap.
6. Fare doppio clic su ogni casella relativa ai nuovi parametri e immettere i valori desiderati.
7. Una volta definiti tutti i valori, è necessario compilare i file dei parametri e dei modelli per creare lo script. Passare alla sezione relativa alla generazione di script.

Creazione e configurazione dei file di ricerca

Questa procedura è facoltativa.

Creazione e configurazione dei file di ricerca

1. Fare clic sulla scheda Servizi di raccolta per visualizzare il pannello contenente l'albero omonimo.
2. Fare clic con il pulsante destro del mouse su un servizio di raccolta, quindi fare clic su Nuovo file di ricerca.
3. Nella casella Nuovo file di ricerca, digitare il nome del nuovo file e premere Invio.
4. Nella colonna della corrispondenza, fare doppio clic su Nuovo, immettere la stringa con cui effettuare il confronto e premere Invio. È possibile aggiungere, inserire ed eliminare le clausole match.
    - Aggiunta: nella colonna della corrispondenza, fare clic su una clausola di corrispondenza, quindi su Aggiungi clausola di corrispondenza.
    - Inserimento: nella colonna della corrispondenza, fare clic su una clausola di corrispondenza, quindi su Inserisci clausola di corrispondenza.

- Eliminazione: nella colonna della corrispondenza, fare clic su una clausola di corrispondenza, quindi su Elimina clausola di corrispondenza.

5. (Operazione facoltativa) Per immettere i comandi di analisi, fare clic con il pulsante destro del mouse sulla colonna dell'analisi per aprire l'editor visuale.
   Per informazioni sull'uso dell'editor visuale, vedere la sezione Immissione dei comandi di analisi mediante l'editor visuale.
6. Scegliere i comandi di analisi e completarli nella finestra dell'editor di comandi.
   I comandi vengono visualizzati nella colonna dell'analisi
7. Una volta definiti tutti i valori, è necessario compilare il file per creare lo script.
   Passare alla sezione Generazione dello script.

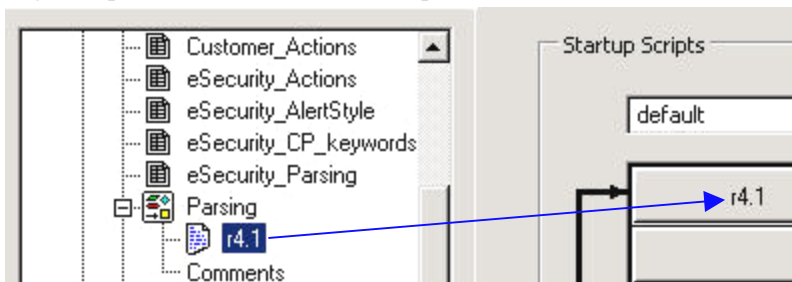
Script

Gli script vengono generati dai modelli. Da un modello è possibile generare più script. La Gestione servizi di raccolta consente di:

- Generare uno script
- Eseguire il debug di uno script
- Assegnare una sequenza di avvio a uno script

Generazione dello script

Generazione di uno script

1. Fare clic sulla scheda Servizi di raccolta per visualizzare il pannello contenente l'albero omonimo.
2. Nel pannello sinistro, selezionare il modello da cui si desidera generare gli script.
3. Fare clic su File > Genera script.
4. Nella scheda dell'editor di modelli, trascinare uno script dal modello alla colonna degli script di avvio o di backout del pannello destro.

Gli script vengono eseguiti nell'ordine in cui appaiono nelle colonne degli script di avvio e di backout. Per modificare l'ordine degli script, trascinarli verso l'alto o il basso all'interno delle colonne.

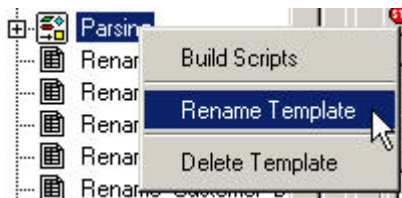
NOTA: l'ultimo script di una sequenza di backout deve terminare con lo stato di elaborazione Arresto.

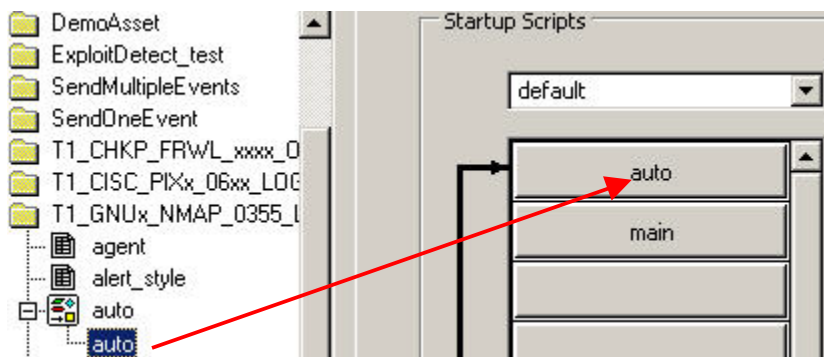
5. (Operazione facoltativa) Effettuare il debug mediante il debugger.
6. Fare clic su File > Salva.
7. Affinché le modifiche diventino effettive, arrestare e avviare la porta mediante gli appositi pulsanti sulla barra degli strumenti.

Attivazione della generazione automatica per i servizi di raccolta precedenti alla versione 5.0

L'attivazione della funzione di generazione automatica consente di non eseguire l'operazione di creazione degli script durante la configurazione e la distribuzione dei servizi di raccolta.

Attivazione della funzione di generazione automatica per i servizi di raccolta precedenti alla versione 5.0

1. Copiare i file seguenti da un servizio di raccolta in versione 5.* esistente e inserirli nel servizio di raccolta per il quale si desidera attivare la funzione di generazione automatica.
   - auto.tem
   - auto.asd
   - auto.lkp
   - auto.par
2. Rinominare il file di modello main.tem. A tale scopo, è possibile utilizzare Generatore serivizi di raccolta.

3. Evidenziare il file del modello rinominato e fare clic sulla scheda Parametri. Modificare in main il nome dell'intestazione della colonna corrispondente quello dello script corrente (ad esempio r4.1) e premere Invio.

4. Fare clic sul pulsante Save (Salva).
5. Nella catena di avvio, fare clic con il pulsante destro del mouse e trascinare il file auto.asd prima di main.

Debug di uno script

All’inizio della procedura di debug, nel pannello Informazioni sulla porta lo stato della porta passa a “Debug”. Per effettuare il debug degli script, consultare il Capitolo 2 relativo al debug delle porte Wizard.

Assegnazione di una sequenza di avvio agli script

Se si desidera che una porta venga attivata all’avvio, È possibile assegnare una sequenza di avvio in modo da eseguire una determinata serie di script. La sequenza di avvio è un file che contiene i nomi degli script da eseguire all’avvio.

Assegnazione di una sequenza di avvio agli script

1. Fare clic con il pulsante destro del mouse sul nome dello script interessato nell’albero dei servizi di raccolta e selezionare Nuova sequenza di avvio. Viene visualizzata la finestra di dialogo Nuova sequenza di avvio.
2. Digitare il nome della sequenza nella finestra di dialogo e fare clic su OK. La sequenza di avvio è un file che contiene i nomi degli script da eseguire all’avvio. I nomi delle sequenze sono soggetti alle limitazioni seguenti:
   - Non è possibile utilizzare "startup" e "backout"
   - Non è possibile utilizzare un nome di sequenza più volte nello stesso servizio di raccolta
3. Trascinare i nomi dei file di script dall’albero dei servizi di raccolta nella colonna degli script di avvio. Gli script vengono eseguiti nell’ordine in cui appaiono nella colonna, dall’alto verso il basso.
4. Per modificare l’ordine degli script, trascinarli all’interno dalla colonna oppure fare clic con il pulsante destro del mouse su Script di avvio e scegliere l'opzione per riordinarli.

Creazione di una porta Wizard

È possibile creare più porte per un servizio di raccolta. Per alcuni tipi di sensore può essere necessario creare più istanze dello stesso servizio di raccolta e assegnare ogni istanza a una porta diversa.

Il tipo di connessione della porta determina quali informazioni vengono acquisite, le modalità con cui viene effettuata questa operazione nonché il momento in cui viene stabilita una connessione. I tipi di connessione sono i seguenti:

- Seriale
- Socket
- File - nuovi

- File - tutti
- Processo permanente
- Processo transitorio
- Trap SNMP
- Nessuna

Connessione seriale

La connessione seriale viene utilizzata se i dati vengono acquisiti da una porta seriale RS-232C (mediante un cavo seriale o un collegamento tramite modem). È necessario indicare la porta seriale interessata (ad esempio COM1, COM2) nella casella Rx/Tx Value (Valore Rx/Tx). Anche l'host che esegue il prodotto che si intende monitorare deve disporre di una connessione seriale all'host del servizio di raccolta, realizzata direttamente mediante un cavo seriale oppure tramite modem a ogni estremità della connessione.

Quando si utilizza questo tipo di connessione, potrebbe essere necessario effettuare altre modifiche o integrazioni.

Connessione socket

La connessione socket viene utilizzata se i dati vengono acquisiti da un socket TCP. È necessario indicare l'indirizzo IP e il numero della porta TCP dell'host remoto nella casella Rx/Tx Value (Valore Rx/Tx), separati dai due punti. Ad esempio, per indicare la porta SMTP è necessario immettere le indicazioni seguenti nella casella Rx/Tx Value (Valore Rx/Tx).

```
<Indirizzo IP>:<porta>
```

Può inoltre essere necessario creare nell'host remoto un processo server per il socket TCP e configurarlo in modo che invii i dati alla porta TCP.

Per ulteriori informazioni sulla configurazione dei servizi di raccolta che utilizzano questo tipo di connessione, consultare la relativa documentazione (ad esempio, Snort, Cisco PIX e Solaris Syslog per i servizi di raccolta) disponibile in

```
%workbench_home%\elements\<nome servizio di
   raccolta>\docs
```

Connessione file - nuovi

La connessione file – nuovi viene utilizzata per acquisire unicamente i dati relativi agli eventi di sicurezza aggiunti al file dopo l'avvio dello script. La connessione apre il file e legge a partire dalla fine. È necessario indicare il percorso del file di log nella casella Rx/Tx Value (Valore Rx/Tx).

Per ulteriori informazioni sulla configurazione dei servizi di raccolta che utilizzano questo tipo di connessione, consultare la relativa documentazione (ad esempio, Solaris Syslog per i servizi di raccolta) disponibile in

```
%workbench_home%\elements\<nome servizio di
   raccolta>\docs
```

Connessione file - tutti

La connessione file – tutti viene utilizzata per acquisire tutti i dati relativi agli eventi di sicurezza contenuti in un file.

Selezionando le connessioni file – nuovi e file – tutti è possibile immettere "inputfile" o "outputfile" nella casella Rx/Tx Value (Valore Rx/Tx). Il formato è il seguente:

```
inputfile, outputfile
```

oppure

```
inputfile
```

oppure

```
outputfile
```

Se si seleziona la connessione file – nuovi o file – tutti e le dimensioni del file diminuiscono, il file stesso viene letto dall'inizio.

Per ulteriori informazioni sulla configurazione dei servizi di raccolta che utilizzano questo tipo di connessione, consultare la relativa documentazione (ad esempio, Solaris Syslog per i servizi di raccolta e registro eventi di Windows 2000) disponibile in

```
%workbench_home%\elements\<nome servizio di
   raccolta>\docs
```

Connessione processo permanente

La connessione processo permanente viene utilizzata per attivare un processo permanente all'avvio della porta. Il processo comunica con il servizio di raccolta assegnato alla porta e con un'applicazione esterna, ricevendo e trasmettendo gli stati.

I processi permanenti iniziano in corrispondenza del primo stato di lettura/scrittura, vengono eseguiti per tutto il tempo in cui la porta rimane attiva e vengono terminati dalla relativa porta, nell'ambito della procedura di arresto. al termine della quale viene inviato un evento di livello 5. All'avvio della porta, invece, viene inviato un evento di livello 1.

Per ulteriori informazioni, consultare la sezione Processi permanenti e transitori. Per informazioni sull'impostazione del valore Rx/Tx per questo tipo di connessione, consultare la sezione Impostazione del valore Rx/Tx per connessioni permanenti e transitorie (Rx/Tx Type (Tipo Rx/Tx)). Per ulteriori informazioni sulla configurazione dei servizi di raccolta che utilizzano connessioni permanenti, consultare la relativa documentazione (ad esempio, Firewall e VPN Check Point per i servizi di raccolta) disponibile in

```
%workbench_home%\elements\<nome servizio di
   raccolta>\docs
```

Connessione processo transitorio

La connessione processo transitorio viene utilizzata per attivare un processo transitorio all'avvio della porta. Il processo comunica con il servizio di raccolta assegnato alla porta e con un'applicazione esterna, ricevendo e trasmettendo gli stati.

I processi transitori possono venire avviati più volte e vengono terminati dalla relativa porta, nell'ambito della procedura di arresto.

NOTA: se si seleziona la connessione per processi permanenti o transitori, è necessario che il valore Rx/Tx comprenda il percorso e il nome del file relativi al processo da eseguire. È possibile utilizzare percorsi e nomi di file completi oppure relativi (rispetto a %WORKBENCH_HOME%). Ad esempio:

```
Percorso completo:
C:\Programmi\Cisco\Csids_client - start
Percorso relativo:
```

```
.\elements\Cisco\Csids_client - start
```

Nel caso dei processi permanenti, si presume che il valore Rx/Tx sia relativo, a meno che non sia indicato un percorso completo.

Terminazione dei processi transitori: se un processo transitorio si interrompe prima della terminazione dell'analizzatore sintattico, esso viene riavviato in occasione dell'invio dello stato di lettura o scrittura successivo privo di eventi.

Per ulteriori informazioni, consultare la sezione Processi permanenti e transitori. Per informazioni sull'impostazione del valore Rx/Tx per questo tipo di connessione, consultare la sezione Impostazione del valore Rx/Tx per connessioni permanenti e transitorie (Rx/Tx Type (Tipo Rx/Tx)).

Connessione trap SNMP

La connessione trap SNMP viene utilizzata per ricevere trap SNMP v1, v2 e v3 inviati dai sensori all'indirizzo IP del server Wizard. In base all'indirizzo IP e all'identificatore dell'oggetto (IDO) del dispositivo che effettua l'invio, la funzione Gestione servizi di raccolta attiva l'analisi per mezzo del servizio di raccolta appropriato. Lo stato Rx (analisi) inoltra i dati dei trap SNMP interni al servizio di raccolta.

È possibile configurare tutte le informazioni utilizzate per raccogliere e analizzare i trap SNMP v1 e v3:

- I trap SNMP v1 sono identificati mediante l'indirizzo IP e l'identificatore dell'oggetto (IDO) nonché tramite il codice trap.
- I trap SNMP v2/v3 sono identificati mediante l'indirizzo IP, il nome di sicurezza, l'ID del motore, le chiavi di autenticazione e di cifratura (se abilitate nel trap) e l'identificatore dell'oggetto (IDO).

Il formato originale del trap, in termini di valori, viene mantenuto il più possibile inalterato. Esso è normalmente definito nel MIB (database delle informazioni di gestione) relativo al sensore da cui è originato l'evento.

Per ulteriori informazioni, vedere Impostazione di trap SNMP.

Tipo di connessione "nessuno"

Questa impostazione viene utilizzata in assenza di porte di comunicazione ed è più efficiente poiché non tenta di effettuare alcuna connessione. Il suo impiego è necessario quando un servizio di raccolta non utilizza lo stato di ricezione e si limita a elaborare i comandi.

Per ulteriori informazioni sull'impostazione dei servizi di raccolta che non utilizzano alcuna connessione, consultare la relativa documentazione (ad esempio, ISS RealSecure e ISS SiteProtector per i servizi di raccolta) disponibile in

```
%workbench_home%\elements\<nome servizio di
   raccolta>\docs
```

Creazione, assegnazione, avvio e arresto di porte Wizard

Creazione di porte Wizard

1. Per informazioni sulla configurazione del servizio di raccolta, consultare la documentazione del servizio di raccolta disponibile in %workbench_home%\elements\<nome servizio di raccolta>\docs.
2. Fare clic sulla scheda Servizi di raccolta e selezionare un servizio.

3. Nel Generatore servizi di raccolta, fare clic sulla scheda Host Wizard.
4. Nel pannello Informazioni sulla porta situato sul lato destro, fare doppio clic su Nuovo, digitare il nome della porta e premere Invio.
5. Scegliere un tipo Rx/Tx.
6. Specificare le opzioni di configurazione in base al tipo di connessione selezionato:
   - Per le connessioni seriali e socket: nella casella relativa al nome della porta, fare clic su quest'ultimo e scegliere Edit Rx/Tx Value (Modifica valore Rx/Tx). Indicare una selle serie di opzioni seguenti:
     - Per le connessioni seriali: scegliere velocità di trasmissione, dimensioni della parola e bit di start e di stop. Fare clic su OK.
     - Per le connessioni socket: immettere l'indirizzo IP e il numero della porta del computer host, separati da due punti. Se non si intende utilizzare lo stato di ricezione, impostare il tipo su Nessuno e fare clic su OK.
   - Per tutte le altre connessioni: fare doppio clic sulla cella Rx/Tx Value (Valore Rx/Tx), immettere le informazioni necessarie e premere Invio.
   - Per le connessioni trap SNMP, vedere Impostazione di trap SNMP.
7. Fare doppio clic sulla cella dei servizi di raccolta e scegliere il nome del servizio.
8. Fare clic sull'opzione Port Name (Nome porta), quindi su Other Port Options (Altre opzioni porta). viene visualizzata la finestra di dialogo Other Port Options (Altre opzioni porta).
9. Selezionare o deselezionare la casella di controllo Run Port at Startup (Esegui porta all'avvio), scegliere la sequenza di avvio e fare clic su OK.
10. Se si sta creando una porta per l'host locale, fare clic su File > Salva e deselezionare l'opzione Informazioni sulla porta.

    Se si sta creando una porta per un host remoto, fare clic su File > Carica/Scarica.

    La porta viene aggiunta al pannello Informazioni sulla porta. Per implementare la nuova porta non è necessario riavviare il sistema. Fare clic su Avvio per modificare lo stato della nuova porta da Disattivo ad Attivo.

Processi permanenti e transitori

Grazie ai processi permanenti e transitori, Wizard è in grado di interagire con altre applicazioni per mezzo di script che ricevono o trasmettono dati e risposte alle analisi. Ogni script viene eseguito su una porta diversa, ognuna collegata a una determinata applicazione.

NOTA: le applicazioni sono specificate nella casella Rx/Tx Value (Valore Rx/Tx).

I nomi dei processi possono contenere:

- Spazi
- Barre e barre rovesciate (per gestire vari sistemi operativi)
- Argomenti di comandi
- Percorsi assoluti e relativi (la variabile di ambiente WORKBENCH_HOME è considerata la HOME relativa)

Quando si verifica uno stato di ricezione/trasmissione (Rx/Tx), viene attivato il processo indicato nella casella Rx/Tx Value (Valore Rx/Tx). Il processo termina insieme all'analizzatore sintattico.

Al termine dei processi permanenti viene inviato un evento di livello 5. All'avvio dei processi permanenti viene inviato un evento di livello 1.

L'output standard (stdout) dei processi permanenti/transitori è collegato allo stato "lettura" (ricezione) dell'analizzatore sintattico. L'input standard (stdin) dei processi permanenti/transitori è collegato allo stato "scrittura" (trasmissione) dell'analizzatore sintattico.

Configurazione del valore Rx/Tx per le connessioni permanenti e transitorie (Rx/Tx Type (Tipo Rx/Tx))

Per la configurazione delle connessioni permanenti e transitorie sono disponibili tre processi relativi ai connettori ovvero:

- DBConnector (connettore di processi JDBC)
- Lea Client
- Remote Data Exchange Protocol (RDEP)

Non utilizzare virgolette nella casella Rx/Tx Value (Valore Rx/Tx) nel caso di processi permanenti e transitori. Se il processo è rappresentato da un percorso assoluto a un nome di eseguibile lungo e contenente spazi, è necessario immetterlo senza virgolette. Ad esempio:

```
%WORKBENCH_HOME%\e-security\elements\checkpoint\lea_clien
   t checkpoint\lea_client.conf -new
```

Non utilizzare spazi negli argomenti dell'eseguibile nella casella Rx/Tx Value (Valore Rx/Tx). Questi argomenti sono infatti così delimitati e, in presenza di spazi, il software presume che vi siano due argomenti dove invece ve n'è uno solo. Se gli argomenti passano nella posizione di un file di configurazione, come nel caso di Check Point, utilizzare un percorso relativo rispetto a %WORKBENCH_HOME%. Ad esempio:

```
checkpoint/\lea_client checkpoint/\lea_client.conf -new
```

DBConnector

DBConnector (un connettore di processi JDBC) esegue un client che effettua il collegamento a un server di database, effettua un'interrogazione SQL su di esso e invia il risultato all'output standard nel formato basato su coppie nome-valore. L'interrogazione SQL da eseguire viene letta dall'input standard o da un file. Il nome nel risultato dato dalla coppia nome-valore viene dedotto dal nome della colonna della serie di risultati. Per questo motivo, è necessario indicare esplicitamente il nome della colonna desiderata nell'interrogazione SQL. La sintassi effettiva varia in base al server di database.

Questa applicazione è installata insieme al Gestore servizi di raccolta nella directory $WORKBENCH_HOME/dbconnector.

Per ulteriori informazioni sull'utilizzo di DBConnector, consultare il file README fornito con l'applicazione, la documentazione dei servizi di raccolta di Sentinel per Entercept Host IDS 4.0 (tramite JDBC) oppure visitare il portale del servizio clienti di eSecurity all'indirizzo http://www.esecurityinc.com (in lingua inglese).

Lea Client

Il processo lea_client di Sentinel utilizza l'API Log Export di OPSEC per ricavare i dati da Firewall-1 di Check Point e li restituisce nel formato nome-valore. Il processo lea_client è di norma utilizzato per inviare i dati al servizio di raccolta di Firewall-1 di Check Point

per Sentinel, che provvede alla loro normalizzazione e, in base all'azione dell'evento (ad esempio, interrompere, rifiutare o accettare), invia un avviso al server Sentinel.

Questa applicazione è installata insieme al Gestore servizi di raccolta nella directory $WORKBENCH_HOME/checkpoint.

Per ulteriori informazioni sull'utilizzo del processo lea_client di Check Point, consultare il file README fornito con l'applicazione, la documentazione dei servizi di raccolta di Sentinel per il servizio di raccolta di Firewall e VPN di Check Point (tramite OPSEC) oppure visitare il portale del servizio clienti di eSecurity all'indirizzo http://www.esecurityinc.com (in lingua inglese).

Remote Data Exchange Protocol (RDEP)

Il processo rdep_client è un'applicazione Java che ricava i dati dai sensori remoti Cisco IDS v4.0 che eseguono RDEP. Il processo rdep_client si collega al sensore IDS remoto per mezzo di una connessione HTTP o HTTPS. Una volta effettuato il collegamento, il client apre una sottoscrizione o ne utilizza una esistente. La sottoscrizione descrive il tipo di dati che il sensore IDS deve inviare al client; nel caso di una nuova sottoscrizione, il tipo di dati recuperati può essere variato modificando il file di configurazione di rdep_client. Utilizzando la sottoscrizione, il client invia la richiesta dei dati degli eventi provenienti dal sensore IDS. Il sensore IDS restituisce questi dati in formato XML, convertiti in coppie nome-valore dal client RDEP di Sentinel e analizzati e normalizzati dal servizio di raccolta. Quest'ultimo invia infine l'evento normalizzato a Sentinel.

Questa applicazione è installata insieme al Gestore servizi di raccolta nella directory $WORKBENCH_HOME/cisco/rdep_client.

Per ulteriori informazioni su RDEP, consultare il file README fornito con l'applicazione, la documentazione dei servizi di raccolta di Sentinel per il servizio di raccolta CISCO IDS 4.0 (tramite RDEP) oppure visitare il portale del servizio clienti di eSecurity all'indirizzo http://www.esecurityinc.com (in lingua inglese).

Impostazione di trap SNMP

Sentinel è in grado di ricevere trapSNMP che rappresentano eventi relativi alla sicurezza che si verificano in un sensore appartenente a una determinata rete. Questi eventi vengono inviati a Sentinel attraverso una rete, per mezzo del protocollo SNMP. Il sistema supporta SNMP v1m v2 e v3. Per abilitare Sentinel alla ricezione dei trap SNMP è necessario creare un servizio di raccolta Wizard che utilizzi una connessione di tipo trap SNMP (Rx/Tx).

È possibile configurare le impostazioni del trap SNMP e specificare i parametri che consentono ai servizi di raccolta SNMP di Wizard di trasferire i trap a Sentinel sotto forma di eventi binari.

La finestra per l'impostazione dei trap SNMP consente di configurare le impostazioni dei servizi di raccolta SNMP di Wizard, compresa la porta utilizzata per i trap SNMP, i codici trap e le informazioni relative all'autenticazione e alla cifratura.

Accesso alla finestra dei trap SNMP

1. Nel Generatore servizi di raccolta, assegnare un nome di porta al servizio di raccolta SNMP.
2. Nella casella Rx/Tx Type (Tipo Rx/Tx), scegliere trap SNMP.
3. Fare clic con il pulsante destro del mouse sul nome della porta e scegliere Edit Rx/Tx Value (Modifica valore Rx/Tx).

4. Immettere le informazioni relative a SNMP.

NOTA: la porta trap UDP di default è la 162. Accertarsi che questa porta sia disponibile e, in caso contrario, sceglierne un’altra.

NOTA: a differenza delle altre porte dei servizi di raccolta, il campo Rx/Tx Value (Valore Rx/Tx) viene popolato in base alle impostazioni effettuate nella finestra SNMP Trap Setup (Impostazione trap SNMP). Nel caso dei servizi di raccolta SNMP, pertanto, non è possibile modificare manualmente il campo Rx/Tx Value (Valore Rx/Tx).

5. Salvare e caricare il servizio di raccolta SNMP.
6. Attivare il servizio di raccolta interrompendo e riavviando la funzione Gestione servizi di raccolta.

NOTA: per attivare questo servizio di raccolta, è necessario arrestare e riavviare la funzione Gestione servizi di raccolta come indicato nel passaggio 6.

L'impostazione SNMP è costituita da:

- Indirizzo/i IP del servizio di raccolta
- Versione SNMP
- Porta trap UDP
- Impostazioni SNMP v1
  - Enterprise OID(s) (IDO aziendali)
  - Trap Code(s) (Codici trap)
- Impostazioni SNMP v2/v3
  - Nomi di sicurezza

- Autenticazione
- Chiave di autenticazione
- Cifratura
- Chiave di cifratura
- ID motore con pulsante interrogazione
- IDO trap

La finestra di dialogo SNMP Trap Setup (Impostazione trap SNMP) (aperta facendo clic con il pulsante destro del mouse sul pannello Informazioni sulla porta del Generatore servizi di raccolta e, quindi, facendo clic su Edit Rx/Tx Value (Modifica valore Rx/Tx)) consente di configurare Wizard affinché:

- Riceva i trap su porte diverse dalla porta UDP 162 (default).
- Crei un solo script di analisi di Wizard per l'elaborazione di trap provenienti da più indirizzi IP con informazioni quali vari codici trap e identificatori di oggetti (IDO) trap.
- Consenta l'individuazione di espressioni regolari POSIX in relazione a indirizzi IP, identificatori di oggetti (IDO) aziendali, codici trap e campi IDO trap.
- Una volta decodificati i trap, Wizard imposta i valori delle variabili comprese nello script.

Indirizzi IP del servizio di raccolta

Gli indirizzi IP del servizio di raccolta sono quelli ai quali si desidera ricevere i trap. È possibile indicare più valori, separandoli con un punto e virgola (;). È possibile inoltre utilizzare il formato =<espressione> per individuare le espressioni regolari conformi a POSIX. L'asterisco (*) è un modificatore del carattere o dell'espressione precedente e, nel caso delle espressioni regolari, il punto (.) può essere utilizzato come carattere jolly ovunque della stringa.

Le espressioni regolari più comunemente utilizzate sono le seguenti:

=	individua qualsiasi sequenza di caratteri, indipendentemente dalla lunghezza
= 192\.168.*	individua qualsiasi sequenza di caratteri contenente 192.168 Per individuare le sequenze che presentano un determinato inizio, utilizzare ^192.168... dove ^ è il delimitatore della parte iniziale. Per individuare le sequenze che presentano una determinata fine, utilizzare 0.47$... dove $ è il delimitatore della parte finale.
= [abc]	Individua "a" o "b" o "c".
= [a-zA-Z0-9]	Individua ogni carattere dell'alfabeto (maiuscolo o minuscolo) e qualsiasi cifra fra 0 e 9.

In pratica, dagli esempi precedenti di espressioni regolari è possibile dedurre le regole seguenti:

.	corrisponde a un carattere qualsiasi
*	corrisponde a nessuna o più occorrenze della sequenza precedente
[]	corrisponde a ogni carattere della sequenza tra parentesi

NOTA: è possibile combinare le regole precedenti.

Versione SNMP

È possibile configurare una sola versione SNMP. Le opzioni nei pannelli SNMP v1 Settings (Impostazioni SNMP v1) e SNMP v2/v3 Settings (Impostazioni SNMP v2/v3) vengono abilitate in base alla versione selezionata.

Porta trap UDP

La porta UDP di destinazione di default è la 162.

Impostazioni SNMP v1

Queste impostazioni sono abilitate unicamente se nell'elenco SNMP Version (Versione SNMP) è stato selezionato SNMP v1.

- Enterprise OID(s) (IDO aziendali): identificatori degli oggetti utilizzati per determinare il tipo di servizio di raccolta che ha inviato il trap. È possibile indicare più valori, separandoli con un punto e virgola (;).
- Trap Code(s) (Codice trap): codici trap per i sensori che inviano i trap SNMP. Questi codici rappresentano i tipi di trap inviati da un determinato servizio di raccolta SNMP. È possibile indicare più valori, separandoli con un punto e virgola (;).

Impostazioni SNMP v2/v3

- Security Name(s) (Nome di sicurezza): nome utente impiegato per accedere al servizio di raccolta. I nomi di sicurezza prevedono la distinzione tra maiuscole e minuscole. È possibile indicare più valori, separandoli con un punto e virgola (;).
- Autenticazione: metodo utilizzato per l’autenticazione. I valori disponibili sono:
  - Nessuno: non viene effettuata alcuna autenticazione dei trap SNMP v3.
  - MD5: il nome di sicurezza è configurato in modo da utilizzare l’algoritmo MD5 per creare una firma digitale per l’autenticazione.
- Chiave di autenticazione: password utilizzata per effettuare l’autenticazione dell’utente nel servizio di raccolta. Abilitata solo se l'autenticazione è MD5. Deve essere costituita almeno da otto caratteri. Per le chiavi di autenticazione viene fatta distinzione tra maiuscole e minuscole. È necessario configurare la stessa chiave nel servizio di raccolta SNMP che effettua l’invio.
- Cifratura: metodo utilizzato per la cifratura. I valori disponibili sono:
  - Nessuno: non viene effettuata alcuna cifratura dei trap SNMP v3
  - DES: il sistema si predispone a ricevere trap cifrati con il metodo DES (Data Encryption Standard).
- Chiave di cifratura: chiave utilizzata per decifrare i trap inviati ai servizi di raccolta di Wizard. Deve essere costituita almeno da otto caratteri. Per la chiave di cifratura viene fatta distinzione tra maiuscole e minuscole. È attivata solo quando viene selezionato il metodo DES nell'elenco Cifratura.
- Engine ID(s) (ID motore): identificatore unico associato a un servizio di raccolta SNMP v3. Il pulsante Engine ID Query (Individua ID motore) consente di determinare l’indirizzo IP su cui si desidera effettuare un'interrogazione. Un'interrogazione corretta restituisce le informazioni e aggiunge l'ID del motore. Se nella casella è già presente un ID, ne viene aggiunto uno nuovo a quest'ultimo.
- Trap OID(s) (IDO trap): ID dell’oggetto trap che identifica il tipo di trap ricevuto.

NOTA: in caso di più nomi di sicurezza e ID dei motori, vengono utilizzati gli stessi schemi di autenticazione e di cifratura per tutti.

NOTA: qualora siano necessarie chiavi di autenticazione e di cifratura diverse per i vari servizi di raccolta SNMP, è necessario configurare una porta per ogni servizio.

Variabili trap SNMP

Alcune variabili sono valide per tutti t trap (SNMP v1 e v3), mentre altre sono valide solo per una versione. Le tabelle seguenti riportano tutte le variabili trap, raggruppate in base alla versione di SNMP per la quale è possibile utilizzarle.

- Variabili trap SNMP per SNMP v1 e v3
- Variabili trap SNMP per SNMP v1
- Variabili trap SNMP per SNMP v3

Variabili trap SNMP per SNMP v1 e v3

Variabile	Descrizione
s_Trap_IP	Indirizzo IP del servizio di raccolta/sensore che ha inviato il trap.
s_Trap_Time	Valore relativo al tempo di attività riportato dal servizio di raccolta/sensore che ha inviato il trap. Di norma si tratta del tempo per il quale il servizio di raccolta è stato eseguito. Formato: G:HH:MM:SS.ss (giorni, ore, minuti, secondi, centesimi di secondo).
i_Trap_Version	Valore relativo alla versione: 1 = SNMP v1 3 = SNMP v3
i_Trap_Vars	Numero di associazioni di variabili nel trap.
s_Trap_OID[]	Array (avente dimensioni “i_Trap_Vars”) dei nomi delle variabili MIB associate nel messaggio trap. Ogni elemento dell’array s_Trap_OID è un IDO, ad esempio “.1.3.6.1.4.1.4286....”
s_Trap_Value[]	Array (avente dimensioni “i_Trap_vars”) dei valori delle variabili MIB associate nel messaggio trap. Gli indici di questo array e di s_Trap_OID corrispondono e, pertanto, s_Trap_OID[0] è il nome di una variabile e s_Trap_Value[0] è il suo valore.

Variabili trap SNMP per SNMP v1

Variabile	Descrizione
s_Trap_Ent	Identificatore dell’oggetto aziendale del servizio di raccolta/sensore che ha inviato il trap.
s_Trap_Code_Generic	Codice generico del trap. I valori disponibili sono: 1-5 = trap standard, definiti da IETF (Internet Engineering Task Force) 6 = trap aziendali specifici (il codice è definito in s_Trap_Code_Specific)

s_Trap_Code_Specific	Codice specifico del trap. È significativo solo se s_Trap_Code_Generic = 6.

Variabili trap SNMP per SNMP v3

Variabile	Descrizione
s_Trap_Engine_ID	ID del motore del servizio di raccolta SNMP v3 che ha inviato il trap.
s_Trap_OID	Identificatore dell'oggetto (IDO) che consente di individuare il tipo di trap SNMP v3 ricevuto. Ai fini dell'identificazione dei trap, l'IDO dei trap SNMP v3 sostituisce l'IDO aziendale e i codici trap generici/specifici di SNMP v1.
s_Trap_Security_Name	Nome di sicurezza con il quale è conosciuto il servizio di raccolta SNMP v3 che ha inviato il trap.

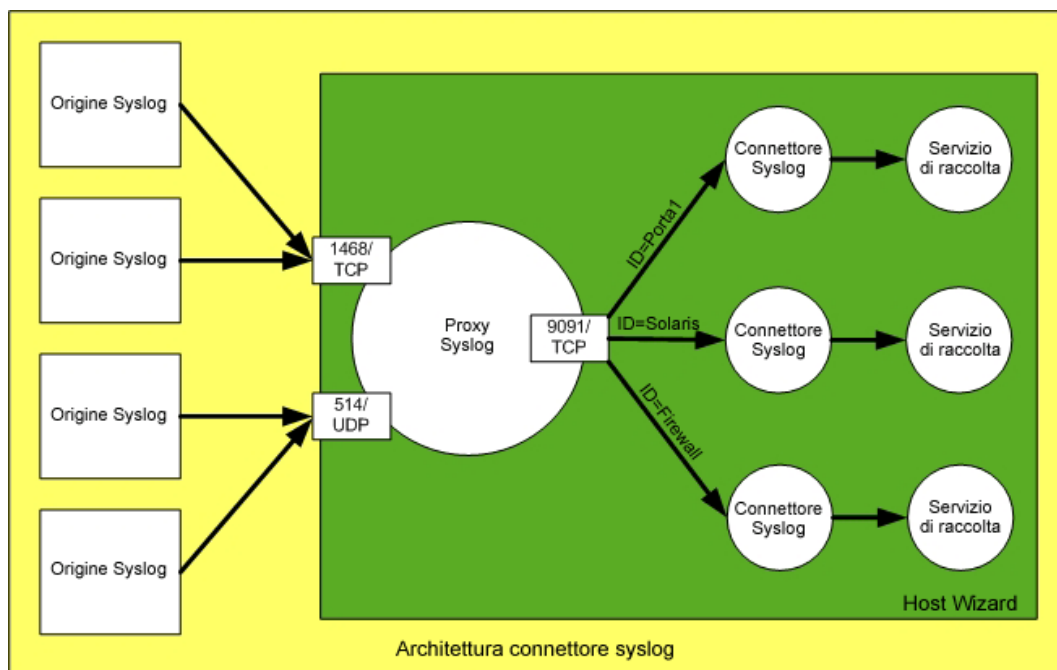
Connettore syslog v1.0.2

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Novell ha rilasciato il connettore syslog per agevolare l'integrazione tra i servizi di raccolta di Sentinel e i prodotti che generano messaggi syslog. In questo documento vengono illustrati architettura, installazione, utilizzo e opzioni del connettore syslog.

Architettura

Il connettore syslog consiste di due parti: il proxy syslog e il client del connettore syslog. Il proxy syslog ascolta le porte UDP e TCP selezionate. La porta UDP di default è la 514, mentre la porta TCP è la 1468, ossia quella normalmente utilizzata dal firewall PIX Cisco per inviare messaggi mediante il protocollo TCP.

Architettura connettore syslog

Di seguito vengono descritte le funzioni svolte da ogni componente del connettore syslog.

- Proxy syslog
  - Si pone in ascolto della porta UDP e/o TCP per la rilevazione di messaggi syslog.
  - Analizza i messaggi in ingresso alla ricerca di componenti standard dei messaggi syslog (Priorità, Data, Nome host e Messaggio)
  - Qualora l'origine invii messaggi privi dei componenti Priorità, Data o Nome host, si attiene alla RFC 3164 "BSD Syslog Protocol" e inserisce i dati mancanti.

- Una volta determinati i componenti struttura e livello in base ai valori Priorità e Nome host, il proxy pubblica il messaggio alle sessioni del connettore syslog interessate.
  - Qualora la sessione client del connettore syslog venga interrotto, il proxy syslog accoda i messaggi in ingresso per il client in questione per 10 minuti. Questo comportamento assicura che il servizio di raccolta non perda messaggi quando viene riavviato o interrotto temporaneamente.
  - Il proxy syslog si pone in ascolto di una porta TCP, in genere la 9091, per servire le sessioni client del connettore syslog.
- Client del connettore syslog
  - Il connettore viene avviato come processo permanente, le cui opzioni relative al runtime sono contenute nel valore RX/TX.
  - Uno dei parametri di runtime è l'ID. È necessario che l'ID configurato per un determinato connettore syslog sia univoco e quindi non venga assegnato ad altri connettori che si collegano allo stesso proxy syslog.
  - Nel runtime è possibile specificare un filtro per i contenuti per limitare l'ambito di validità dei messaggi inviati al servizio di raccolta.
  - Il connettore syslog effettua un collegamento al servizio client del connettore del proxy.
  - Il connettore syslog registra il proprio ID e il filtro dei contenuti nel proxy syslog.
  - I messaggi associati all'ID dal proxy syslog vengono letti dal connettore e indirizzati all'output standard.
  - Attualmente la struttura e il contenuto dei messaggi vengono passati al servizio di raccolta senza apportare loro alcuna modifica. In futuro, il connettore syslog sarà in grado di formattare i messaggi affinché siano conformi ai requisiti previsti per l'analisi da parte del servizio di raccolta.

Il protocollo syslog è da sempre definito come un protocollo basato su UDP. In mancanza di altre applicazioni/dispositivi in grado di inviare messaggi mediante TCP nonché di uno standard riconosciuto per syslog su TCP, è stato adottato il metodo del firewall PIX Cisco per la terminazione dei messaggi syslog (ritorno a capo + avanzamento riga). In syslog su TCP è necessario identificare il punto di terminazione, poiché non esistono standard definiti né limiti "naturali" che separino i messaggi, mentre nel caso di syslog su UDP i messaggi presentano una terminazione naturale, poiché i pacchetti UDP trasportano ognuno un solo messaggio e sono privi di collegamenti.

Installazione e disinstallazione

Il connettore syslog è stato progettato per essere utilizzato su qualsiasi piattaforma Wizard e, per garantirne la portabilità, entrambi i componenti sono scritti in Java. Di seguito vengono riportati i requisiti hardware e software.

Requisiti del sistema

Software

- Java 1.4.1 o superiore
- Wizard 4.2 o superiore
- Windows (2000/XP/2003), Solaris (8/9), RedHat Enterprise Linux (v3 ES/AS)

Hardware

- 14 MB di RAM aggiuntivi (45 MB di memoria virtuale) per ogni istanza del connettore e del proxy syslog

Installazione

I file relativi ai client del proxy e del connettore syslog vengono installati automaticamente durante l'installazione del servizio di raccolta; i file syslog si trovano nella directory seguente.

Per UNIX:

```
$ESEC_HOME/wizard/syslog
```

Per Windows:

```
%ESEC_HOME%\wizard\syslog
```

La procedura guidata non avvia automaticamente il proxy syslog, se si desidera che ciò avvenga, è necessario installare syslog come servizio attenendosi alle istruzioni seguenti.

Installazione come servizio di Windows (Windows)

NOTA: è possibile installare il proxy syslog come servizio di Windows, affinché venga eseguito automaticamente: per ottenere questo risultato, eseguire i comandi seguenti al prompt dei comandi.

- cd /d "%ESEC_HOME%\wizard\syslog"
- syslog-server.bat install

  Viene creato un servizio di Windows denominato "eSecurity Syslog Server".

Installazione come servizio (UNIX)

NOTA: in UNIX, è possibile installare il proxy syslog come servizio affinché venga eseguito automaticamente all'avvio della macchina; per ottenere questo risultato, eseguire i comandi seguenti.

- Eseguire il login come utente radice.
- Eseguire cd $ESEC_HOME/wizard/syslog
- Eseguire ./syslog-server.sh install

  In questo modo, il proxy syslog viene attivato automaticamente all'avvio della macchina. Per default, il proxy syslog viene eseguito come utente radice; ciň č necessario in quanto esso si collega per default alla porta 514, che richiede i privilegi di questo tipo di utente. Per fare in modo che il proxy syslog si colleghi come un altro utente, modificare lo script /etc/init.d/esyslogserver, accertandosi che il tipo di utente in questione disponga dei privilegi per collegarsi alla porta della quale si pone in ascolto per rilevare il transito dei messaggi. Di seguito si riportano alcuni esempi che consentono di ottenere questo risultato:

  - Utilizzare il comando "sudo" per avviare il proxy syslog, assegnando all'utente "sudo" i privilegi necessari per collegarsi alla porta desiderata.
  - Modificare la configurazione di syslog (syslog.conf) affinché il proxy si colleghi a una porta che non richieda i privilegi dell'utente radice (ad esempio 1024). In questo caso, probabilmente sarà necessario reindirizzare i messaggi inviati alla porta 514 verso la porta sostitutiva selezionata.

Disinstallazione

Per disinstallare il proxy, eseguire i comandi seguenti al prompt dei comandi.

Disinstallazione come servizio di Windows (Windows)

- cd /d "%ESEC_HOME%\wizard\syslog"
- syslog-server.bat remove

Disinstallazione come servizio (UNIX)

Per disinstallare il proxy, eseguire i comandi seguenti.

- Eseguire il login come utente radice.
- Eseguire cd $ESEC_HOME/wizard/syslog
- ./syslog-server.sh remove

Utilizzo

Server proxy Syslog

La procedura guidata non avvia automaticamente il server proxy Syslog: se si desidera che ciò avvenga, è necessario installare syslog come servizio attenendosi alle istruzioni riportate nella sezione relativa all'installazione.

La configurazione del proxy syslog è memorizzata nei file seguenti.

Per UNIX:

```
$ESEC_HOME/wizard/syslog/config/syslog.conf
```

Per Windows:

```
%ESEC_HOME%\wizard\syslog\config\syslog.conf
```

Per default, il proxy syslog viene impostato utilizzando la configurazione seguente:

- Listener sulla porta UDP 514 per i messaggi syslog.
- Listener sulla porta TCP 1468 per i messaggi syslog.
- Listener sulla porta TCP 9091 per i collegamenti del connettore.

È possibile configurare il proxy syslog in modo che si ponga in ascolto di altre porte per ricevere messaggi syslog oppure accettare i collegamenti dei client. Gli switch da utilizzare sono:

-udp <porta>	porta per i messaggi UDP provenienti dai dispositivi; default 514
-tcp <porta>	porta per i collegamenti TCP provenienti dai dispositivi; default 1468
-connector <porta>	porta per i collegamenti TCP provenienti dai connettori; default 9091

Per variare queste impostazioni, modificare la sezione seguente del file syslog.conf.

```
wrapper.app.parameter.3=-tcp
wrapper.app.parameter.4=1468
wrapper.app.parameter.5=-udp
wrapper.app.parameter.6=514
wrapper.app.parameter.7=-connector
wrapper.app.parameter.8=9091
```

Ad esempio, se si desidera modificare le impostazioni delle porte come indicato di seguito:

- Listener sulla porta UDP 4514 per i messaggi syslog.
- Listener sulla porta TCP 4168 per i messaggi syslog.
- Listener sulla porta TCP 4991 per i collegamenti del connettore.

È necessario apportare le seguenti modifiche alla sezione del file syslog.conf riportata in precedenza.

```
wrapper.app.parameter.3=-tcp
wrapper.app.parameter.4=4168
wrapper.app.parameter.5=-udp
wrapper.app.parameter.6=4514
wrapper.app.parameter.7=-connector
wrapper.app.parameter.8=4991
```

Per default, la configurazione del proxy syslog viene impostata in modo da accettare i collegamenti client provenienti da qualsiasi host. Per aumentare la sicurezza, è possibile impostare il proxy syslog in modo che accetti unicamente collegamenti dai client che si trovano nello stesso host. Questa precauzione può rivelarsi utile poiché le comunicazioni tra i connettori dei client e il proxy non prevedono alcun controllo della privacy o degli accessi, né procedure di autenticazione. Per effettuare questa impostazione, utilizzare gli switch seguenti:

`-private`	si pone in ascolto dei collegamenti dei connettori durante il loopback.
`-shared`	si pone in ascolto dei collegamenti dei connettori all'host locale (default).

Lo switch –shared fa in modo che il proxy associ il listener del collegamento client a un socket accessibile agli host remoti.

Per variare queste impostazioni, modificare la sezione seguente del file syslog.conf.

```
wrapper.app.parameter.2=-shared
```

Ad esempio, per consentire unicamente collegamenti client provenienti dallo stesso host, è necessario modificare le impostazioni come indicato di seguito:

```
wrapper.app.parameter.2=-private
```

È possibile configurare il proxy syslog affinché registri tutti i messaggi ricevuti in un file di log. Il formato dei messaggi visualizzato è uguale a quello utilizzato dal proxy syslog per inoltrare i messaggi a un altro server syslog. Di conseguenza, la priorità (<PRI>) utilizzata dal server syslog ricevente per determinare i parametri di struttura e livello viene riportata all'inizio di ogni messaggio. Questo tipo di registrazione viene attivata dallo switch

`-log <nome file>` Nome del file di log in cui effettuare le registrazioni.

Per attivare la registrazione, aggiungere le due righe seguenti al file syslog.conf, dopo l'ultima stringa "wrapper.app.parameter":

```
wrapper.app.parameter.11=-log
wrapper.app.parameter.12=<nome file>
```

Ad esempio, per attivare la registrazione per il file $ESEC_HOME/wizard/syslog/messages.log, modificare le impostazioni come segue:

```
wrapper.app.parameter.7=-connector
wrapper.app.parameter.8=9091
wrapper.app.parameter.9=-messageSize
wrapper.app.parameter.10=5000
wrapper.app.parameter.11=-log
wrapper.app.parameter.12=messages.log
```

Se il nome del file non contiene un percorso assoluto, quello specificato si riferisce alla directory $ESEC_HOME/wizard/syslog.

NOTA: le dimensioni del file di log possono aumentare in modo significativo, quindi è opportuno accertarsi che la posizione dove viene memorizzato il file disponga di abbondante spazio libero (è quindi preferibile utilizzare una directory che non si trovi in $ESEC_HOME).

È consigliabile eseguire il proxy syslog con almeno 64 MB e non oltre 256 MB di memoria heap JVM (Java Virtual Machine). Questa configurazione consente normalmente di ottenere le prestazioni seguenti:

Limiti del server proxy

▪ Numero massimo di eventi	500 eps (in totale, per tutte le porte client)
▪ Dimensioni Q massime del connettore:	5000 messaggi (valore di default, in assenza di altre indicazioni)
▪ Numero massimo di connettori:	5

Per variare le impostazioni della memoria, modificare la sezione seguente del file syslog.conf:

```
# Dimensioni heap Java iniziali (in MB)
wrapper.java.initmemory=64

# Dimensioni massime heap Java (in MB)
wrapper.java.initmemory=256
```

Client del connettore syslog

Il client del connettore syslog effettua il collegamento al proxy syslog raccogliendo i messaggi per i quali ha effettuato la sottoscrizione. I messaggi raccolti dal client vengono quindi trasmessi all'output standard. La sessione instaurata tra il client e il serve non viene interrotta fino a quando il processo client o il proxy syslog non vengono terminati. Questo comportamento rende il client particolarmente adatto per essere utilizzato dal motore del servizio di raccolta in qualità di connettore per processi permanenti.

Nella finestra per la configurazione delle porte del Generatore servizi di raccolta, configurare la porta in questione utilizzando un tipo e un valore Rx/Tx simili ai seguenti.

Per UNIX:

```
syslog/SyslogConnectorAgent.sh <argomenti>
```

Per Windows:

```
syslog\SyslogConnectorAgent.bat <argomenti>
```

Una volta indicato il valore Rx/Tx, scegliere il servizio di raccolta appropriato dalla libreria e caricare la configurazione della porta, ed eventualmente anche il servizio di raccolta stesso, nella procedura guidata remota.

Per semplificarne l'uso generale, il client del connettore syslog è stato progettato in modo da utilizzare vari argomenti di default. La riga di comando più semplice per il client del connettore syslog è la seguente:

Per UNIX:

```
syslog/SyslogConnectorAgent.sh -id "IDUnivoco"
```

Per Windows:

```
syslog\SyslogConnectorAgent.bat -id "IDUnivoco"
```

L'interpretazione della riga di comando è la seguente:

- Collegamento al proxy syslog in ascolto su questa connessione all'indirizzo 127.0.0.1:9091
- Sottoscrizione di tutti i messaggi inviati, indipendentemente dal valore del campo Facilities (Strutture) di syslog
- Sottoscrizione di tutti i messaggi inviati, indipendentemente dal valore del campo Levels (Livelli) di syslog
- Sottoscrizione di tutti i messaggi, indipendentemente dall'indirizzo dell'origine IP contenuta nell'intestazione.
- Sottoscrizione di tutti i messaggi, indipendentemente dall'indicazione dell'host all'interno dei messaggi stessi.
- Assegnazione dell'ID contenuto in "IDUnivoco" ai parametri per la sottoscrizione alla sessione.

La sessione del client del connettore syslog viene registrata all'interno del proxy syslog, insieme con il filtro delle sottoscrizioni descritto in precedenza, facendo riferimento all'ID di "MyUniqueID". L'ID è obbligatorio. L'ID è obbligatorio ed è necessario che sia unico, ovvero che non venga assegnato ad altre sessioni client del connettore che si collegano allo stesso proxy syslog. Qualora venga configurato un altro client del connettore syslog avente lo stesso ID, una delle due connessioni viene eliminata. In particolare, viene mantenuta l'ultima sessione che si è collegata utilizzando l'ID in questione.

Il filtro generico mostrato in precedenza potrebbe vanificare le elaborazioni del servizio di raccolta, qualora i messaggi che soddisfano i requisiti del filtro (e che quindi vengono ricevuti) non siano pertinenti a una determinata operazione del servizio stesso. L'esempio precedente mostra come l'impostazione del filtro sia molto versatile, mentre l'esempio seguente, relativo a UNIX, riporta una descrizione più restrittiva e precisa dei messaggi pertinenti per il servizio di raccolta.

```
syslog/SyslogConnectorAgent.sh -facilities "user,kernel" -
   levels "warning,error" -sender
   "192.16.0.12,192.16.0.0/16" -host
   "17.16.8.0/24,10.1.1.13" -id "MyOtherUniqueID"
```

L'interpretazione della riga di comando è la seguente:

- Collegamento al proxy syslog in ascolto su questa connessione all'indirizzo 127.0.0.1:9091
- (-facilities) Sottoscrizione di tutti i messaggi inviati il cui campo Facilities (Strutture) contenga le parole chiave user o kernel
- (-facilities) Sottoscrizione di tutti i messaggi inviati il cui campo Levels (Livelli) contenga le parole chiave warning o error
- (-sender) Sottoscrizione ai messaggi identificati dall'indirizzo IP di origine associato ai messaggi in ingresso al proxy syslog. Questo argomento fa in modo che il proxy syslog esamini le informazioni contenute nell'intestazione IP in modo da effettuare una valutazione in base ai criteri esposti. Ciò consente al filtro di gestire i relay server syslog, che non forniscono i propri dati identificativi nei messaggi che inoltrano. Sebbene questo argomento sia stato progettato per gestire i messaggi inoltrati, è possibile utilizzarlo per filtrare i messaggi inviati direttamente dall'origine syslog. In particolare, i relay server o origini syslog interessati sono 192.16.0.12 e 192.16.0.0/16, il secondo dei quali in realtà rappresenta un intervallo di indirizzi IP; pertanto, se l'indirizzo IP dell'origine è compreso tra 192.16.0.0 e 192.16.255.255, i messaggi inviati sono conformi ai criteri del filtro. I nomi host non sono ammessi, poiché non viene effettuata alcuna risoluzione per determinare il nome host corrispondente agli indirizzi IP delle origini.
- (-host) Sottoscrizione ai messaggi che contengono gli indicatori di host 17.16.8.0/24 o 10.1.1.13 all'interno del messaggio syslog. Il primo elemento è un intervallo di indirizzi IP. I messaggi che contengono un indicatore di host sotto forma di indirizzo IP compreso tra 17.16.8.0 e 17.16.8.255 soddisfano la condizione impostata nel filtro. I nomi di host sono supportati dall'argomento -host ed è possibile indicarli letteralmente oppure mediante espressioni regolari ricordando che, anche nel caso di questo argomento, non viene effettuata alcuna risoluzione dei nomi host. Pertanto, qualora si configuri un nome host o un indirizzo IP il filtro non sarà in grado di gestire l'altro schema di assegnazione dei nomi. Ad esempio, impostando -host 172.16.0.90 non vengono identificate corrispondenze con i criteri del filtro in un messaggio contenente il nome host "testbox1", anche nel caso in cui i servizi di risoluzione dei nomi prevedano l'associazione tra 172.19.0.90 e "testbox1". Quindi, l'indicazione IP degli host consente di gestire unicamente indirizzi IP, mentre l'indicazione dei nomi host consente di gestire esclusivamente questi ultimi.

Il filtro menzionato nell'esempio precedente può essere descritto per mezzo dell'espressione booleana seguente:

```
(Facility="user" o Facility="kernel") e (Level="warning"
   o Level="error") e (Sender="192.16.0.12"
   o Sender=192.16.0.0/16") e (Host="17.16.8.0/24"
   o Host="10.1.1.13")
```

Il numero delle combinazioni possibili dei vari argomenti corrisponde il prodotto cartesiano dei tipi di argomenti in cui ogni tipo di argomenti costituisce una serie. Secondo PRINCIPIA

CYBERNETICA WEB (http://pespmc1.vub.ac.be/ASC/CARTES_PRODU.html) (in lingua inglese), il prodotto cartesiano è:

> "L'insieme di tutte le n-tuple ordinate che č possibile ottenere giustapponendo un elemento della prima, uno sella seconda e uno dell'n-esima serie. Questo insieme puň essere considerato uno spazio a n dimensioni, nel quale ogni n-tupla indica una cella. Il prodotto cartesiano piů semplice di due serie č una tabella bidimensionale o una tabulazione incrociata le cui celle possono essere utilizzate per immettere frequenze, indicare possibilitŕ (vedere "relazione") o impossibilitŕ (vedere "vincolo"), oppure per tenere traccia delle transizioni che si riferiscono al comportamento di un sistema." (Krippendorff)

NOTA: alla data di pubblicazione di questo documento, l'indirizzo del sito Web risultava corretto.

Ciò significa che, in teoria, un numero elevato di messaggi distinti potrebbe superare questo filtro; Pertanto, il numero di messaggi diversi viene indicato con precisione solo dalle condizioni operative reali.

Oltre a filtrare gli argomenti della riga di comando, è possibile utilizzare gli argomenti seguenti:

`-proxy <indirizzo_server>:<n. porta>`	Indirizzo dell'host del proxy server syslog e numero della porta a cui effettuare il collegamento.
`-log <nome file>`	Consente di effettuare la registrazione nel file indicato.

L'argomento -proxy consente di configurare il client del connettore affinché effettui il collegamento a una porta TCP diversa da quella di default o a un host diverso da quello locale. Per default, il proxy syslog si aspetta che le connessioni dei client avvengano sulla porta 9091. Qualora questa porta non sia disponibile nell'host in cui viene eseguito il proxy syslog, è possibile modificarla all'avvio del proxy stesso e, utilizzando l'argomento –proxy, è possibile fare in modo che i client si colleghino alla nuova porta. È inoltre possibile specificare l'host di destinazione del client del connettore affinché non corrisponda al sistema locale. Qualora il server proxy accetti sessioni di client di connettori remoti, è possibile configurare un client del connettore syslog in modo tale da instaurare una sessione con il proxy syslog remoto in questione. In questo caso, è possibile configurare l'indirizzo IP e la porta del client del connettore del proxy syslog per mezzo dell'argomento –proxy.

L'argomento -log attiva la funzione di registrazione del client del connettore, che invia i messaggi a mano a mano che li riceve dal proxy syslog. A differenza del file di log del proxy syslog, il contenuto dei messaggi viene filtrato in base alle informazioni della sottoscrizione registrata; inoltre i messaggi registrati non contengono il campo <PRI> relativo alla priorità. Il contenuto è quindi coerente con ciò che il servizio di raccolta riceve dallo stesso client del connettore syslog.

NOTA: le dimensioni del file di log possono aumentare in modo significativo, quindi è opportuno accertarsi che la posizione dove viene memorizzato il file disponga di abbondante spazio libero (è quindi preferibile utilizzare una directory che non si trovi in $ESEC_HOME).

Un esempio di utilizzo degli argomenti –proxy e –log in UNIX è il seguente:

```
syslog/SyslogConnectorAgent.sh -proxy localhost:9091 -log
   connector_messages.log -id "IDUnivoco"
```

Configurazione della registrazione per il server proxy syslog

Il server proxy syslog memorizza i messaggi di registrazione nel file

```
$ESEC_HOME/wizard/syslog/syslog_trace*.*.log
```

Modificando il file delle proprietà, è possibile modificare i livelli di registrazione:

```
$ESEC_HOME/wizard/syslog/syslog_log.prop
```

Si tratta del file delle proprietà di registrazione specificato dalla riga seguente del file syslog.conf:

```
wrapper.java.additional.1=-
   Djava.util.logging.config.file=syslog_log.prop
```

Per variare i livelli di registrazione, modificare opportunamente la sezione seguente:

```
###### Configurazione dei livelli di registrazione
# Le regole inerenti alla registrazione vengono lette
   dall'alto verso il basso.  Iniziare con le regole più
   generali e, quindi, passare a quelle più specifiche.
…
######
```

Esempi di argomenti della riga di comando

È possibile eseguire il server proxy syslog e il connettore del client senza utilizzare gli script forniti con l'installazione. A tal fine, è necessario utilizzare gli argomenti della riga di comando descritti in questa sezione.

Proxy syslog:

```
java -server -Xms64m -Xmx256m -
   Djava.util.logging.config.file=syslog-logger.prop -jar
   syslog.jar [-udp <porta>] [-tcp <porta>] [-connector
   <porta>] [-private|-shared] [-log <percorso file>] [-
   messageSize <numero>]
```

Argomenti validi:

-server	È necessario indicarlo sempre, poiché è utilizzato dalla JVM.
-Xms64m	Specifica le dimensioni iniziali della memoria del proxy syslog. È consigliabile impostare 64 MB.
-Xmx256m	Specifica le dimensioni massime della memoria del proxy syslog. Il valore consigliato è pari a 256 MB. Ciò consente

	al server proxy di gestire eventuali picchi nel volume dei dati, più connettori client nonché i buffer creati qualora i connettori ripetano il collegamento. In caso di aumento del volume di dati o del numero di connettori client collegati è possibile aumentare questo valore, a condizione che vi sia memoria disponibile. In ogni caso, esso non può superare 1,2 GB per server proxy syslog ovvero '–Xmx1200m'.
-Djava.util.logging.config.file	Questa proprietà specifica il percorso e il nome del file di configurazione delle registrazioni per il debug; per questo motivo, è necessario che esso faccia riferimento alla posizione in cui si trova il file. Qualora non sia specificato alcun percorso, viene considerata la directory corrente dalla quale è stata eseguita la JVM. Esempio: %workbench_home%\syslog-logger.prop

-udp <porta>	porta per i messaggi UDP provenienti dai dispositivi, default 514
-tcp <porta>	porta per i collegamenti TCP provenienti dai dispositivi, default 1468
-connector <porta>	porta per i collegamenti TCP provenienti dai connettori, default 9091
-private	si pone in ascolto dei collegamenti dei connettori durante il loopback (default).
-shared	si pone in ascolto dei collegamenti dei connettori all'host locale. Se non viene impostato, viene generato un errore di comunicazione.
-log	nome del file di log in cui effettuare le registrazioni.
-help	Genera questo messaggio di guida
-version	Restituisce la versione del proxy (0.91-poc)
-messageSize	Numero di messaggi memorizzati nel buffer, da inviare nuovamente nel caso di collegamenti interrotti temporaneamente. La dimensione massima è pari a 5000 senza virgole. Se non viene indicato alcun valore, oppure se esso è maggiore di 5000, l'argomento viene impostato di default su 5000.

Client del connettore syslog:

```
java -jar syslogconnector.jar -id <IDUnivoco> [-proxy
   <host:numero porta>] [-facilities
   <struttura1,struttura2,…>] [-levels <livello1,
   livello2,…>] [-sender <IP1 di origine[/integer subnet
   mask], IP2 di origine[/integer subnet mask],…>] [-host
   < IP1[/integer subnet mask]|Hostname1 | Hostname
   Regex1, IP2[/integer subnet mask]|Hostname2 | Hostname
   Regex2, …>] [-log <percorso del file di log>]
```

Argomenti validi:

Argomento	Descrizione
`-proxy <host:numero porta>`	Il proxy syslog per effettuare il collegamento all'host e alla porta di default è 127.0.0.1:9091.
`-facilities <struttura1,struttua2,…>`	Elenco separato da virgole delle strutture desiderate; l'impostazione di default comprende tutte le strutture.
`-levels <livello1, livello2,…>`	Elenco separato da virgole dei livelli di gravità desiderati; l'impostazione di default comprende tutti i livelli.
`-sender <IP1 di origine[/integer subnet mask], IP2 di origine[/integer subnet mask],…>`	Elenco separato da virgole dei mittenti desiderati; l'impostazione di default comprende tutti i mittenti.
`-host < IP1[/integer subnet mask]|Hostname1 | Hostname Regex1, IP2[/integer subnet mask`	Elenco separato da virgole degli host desiderati; l'impostazione di default comprende tutti gli host.
`-log <percorso del file di log>`	Nome del file di log in cui effettuare le registrazioni.
`-id <IDUnivoco>`	Consente di indicare l'identità del connettore (OBBLIGATORIO)
`-help`	Genera questo messaggio di guida
`-version`	Restituisce la versione del connettore (0.91-poc)

Tabella delle strutture supportate

Quando il nome delle strutture è specificato nella riga di comando del client del connettore syslog, non viene effettuata alcuna distinzione tra maiuscole e minuscole.

KERNEL	UUCP	LOCAL0
USER	CRON	LOCAL1
MAIL	SECURITY	LOCAL2
DAEMON	FTP DAEMON	LOCAL3
AUTH	NTP	LOCAL4
SYSLOG	LOG AUDIT	LOCAL5
LPR	LOG ALERT	LOCAL6
NEWS	CLOCK DAEMON	LOCAL7

Tabella dei livelli supportati

Quando il nome dei livelli è specificato nella riga di comando del client del connettore syslog, non viene effettuata alcuna distinzione tra maiuscole e minuscole.

EMERGENCY	WARNING
ALERT	NOTICE
CRITICAL	INFORMATIONAL
ERROR	DEBUG

Note sulla distribuzione

Messaggi inoltrati al proxy syslog

La maggior parte dei server syslog è in grado di reindirizzare i messaggi ricevuti a un altro server syslog, nonché di elaborare i messaggi in ingresso. In fase di distribuzione, potrebbe sembrare opportuno modificare un log host per realizzare il reindirizzamento dei messaggi al proxy syslog; tuttavia, il comportamento anomalo di alcuni server syslog rende questa scelta poco adatta alla distribuzione.

È stato osservato che i server syslog di Solaris 7 e 9 nonché di Linux 8 (che possono essere rappresentativi di altre versioni distribuite) non inseriscono il nome dell'host o l'indirizzo IP nei messaggi che inviano all'host. Il server syslog ricevente associa l'indirizzo IP o il nome host (mediante la risoluzione dei nomi) di origine ai file di log che genera. Qualora Solaris 9 inoltri i messaggi al proxy in questione, non inserisce al loro interno l'indirizzo IP o il nome host dell'origine da cui provengono. Questo comportamento è anomalo, poiché il file di log del sistema Solaris 9 mostra un indirizzo IP o un nome host. In assenza del nome host supplementare nel messaggio, il proxy syslog deduce che il messaggio proviene dal relay server e non dall'host originale, aggiungendo a tutti i messaggi ricevuti da Solaris 9 l'indirizzo IP dell'host che ha effettuato l'inoltro. Questo comportamento implica conseguenze significative, poiché il servizio di raccolta e, quindi, Sentinel, non sono in grado di determinare l'origine degli eventi relativi alla sicurezza.

È quindi consigliabile che il proxy non sia il destinatario di messaggi inoltrati qualora questi ultimi non contengano l'indirizzo IP o il nome host dell'origine reale. Qualora il proxy venga utilizzato in produzione, questa indicazione può comportare conseguenze significative sotto il profilo logistico.

Esempio:

Un evento su si verifica in ultrabookIIi (172.16.0.70) che esegue Solaris 7 e inoltra i messaggi a talkabout (172.16.0.72) che esegue Solaris 9 e, a sua volta, inoltra i messaggi al proxy syslog. I seguenti sono i messaggi generati dal connettore Sentinel.

Proxy:

```
<37>Apr 02 06:54:11 [172.16.0.72.151.234] su: 'su root'
   succeeded for oespadm on /dev/pts/0
```

Client del connettore:

```
Apr 02 06:54:11 [172.16.0.72.151.234] su: 'su root'
   succeeded for oespadm on /dev/pts/0
```

Di seguito viene riportata la traccia dei pacchetti relativi al primo messaggio, in occasione dell'arrivo a talkabout e dell'inoltro al server proxy di pes020.esecurity.net.

```
# snoop -x0 udp port 514
Using device /dev/dmfe0 (promiscuous mode)
ultrabookIIi -> talkabout    SYSLOG C port=42830 <37>Apr
   1 18:54:11
```

```
0: 0000 83cd 1395 0040 2082 202b 0800 4500      .......@ .
   +..E.
16: 0061 fa09 4000 ff11 28d3 ac10 0046 ac10
   .aú.@...(....F..
32: 0048 a74e 0202 004d 5d7e 3c33 373e 4170
   .H.N...M]~<37>Ap
48: 7220 2031 2031 383a 3534 3a31 3120 7375    r  1
   18:54:11 su
64: 3a20 2773 7520 726f 6f74 2720 7375 6363    : 'su root'
   succ
80: 6565 6465 6420 666f 7220 6f65 7370 6164    eeded for
   oespad
96: 6d20 6f6e 202f 6465 762f 7074 732f 30      m on
   /dev/pts/0

talkabout -> pes020.esecurity.net SYSLOG C port=38890
   <37>Apr  1 18:54:11

0: 000a 5e02 a335 0000 83cd 1395 0800 4500
   ..^..5........E.
16: 0061 304b 4000 ff11 f031 ac10 0048 ac10
   .a0K@....1...H..
32: 02a6 97ea 0202 004d 6a82 3c33 373e 4170
   .......Mj.<37>Ap
48: 7220 2031 2031 383a 3534 3a31 3120 7375    r  1
   18:54:11 su
64: 3a20 2773 7520 726f 6f74 2720 7375 6363    : 'su root'
   succ
80: 6565 6465 6420 666f 7220 6f65 7370 6164    eeded for
   oespad
96: 6d20 6f6e 202f 6465 762f 7074 732f 30      m on
   /dev/pts/0
```

Il contenuto della registrazione effettuata da talkabout, invece, è il seguente:

```
Apr  1 18:54:11 ultrabookIIi su: 'su root' succeeded for
   oespadm on /dev/pts/0
```

Configurazione di un server socket su host UNIX

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

I server socket rappresentano un punto di terminazione per i collegamenti socket di Gestione servizi di raccolta di Wizard su UNIX. Ad esempio, se si desidera monitorare un file di log o una postazione UNIX mediante una procedura guidata remota, è necessario attraversare un firewall per raggiungere la porta della postazione UNIX in questione.

Le istruzioni seguenti consentono di impostare un server socket in un host UNIX e monitorare un file di log ASCII che si trova al suo interno.

Per impostare un processo relativo a un server socket in un host UNIX

1. Creare lo script che invia i dati al collegamento socket TCP. A tal fine, creare un nuovo file di testo e copiarvi le linee seguenti, sostituendo <file di log> con il percorso completo dei file che si intende monitorare:

   ```
   #!/bin/sh
   /bin/tail -f <file di log>
   ```

   Salvare il file (assegnando un percorso e un nome a piacere) in una posizione dove non venga eliminato e, preferibilmente, utilizzando un nome significativo. Ad esempio:

   ```
   /usr/local/bin/logfileserver
   ```

2. Selezionare una porta TCP dell'host UNIX che non richieda privilegi da destinare all'utilizzo da parte del processo del server. Il numero delle porte che non richiedono privilegi è compreso tra 1025 e 65.535. Per verificare se il numero della porta è già in uso, utilizzare il comando seguente (sostituendo <numero porta> con la porta desiderata):

   ```
   netstat -an | grep LISTEN | grep <numero porta>
   ```

   Se viene restituita una riga (come nell'esempio seguente), la porta è in uso ed è necessario sceglierne un'altra.

   ```
   *.5555*.*0000 LISTEN
   ```

3. Come utente radice, modificare file /etc/services e aggiungere una voce per il nuovo servizio socket alla fine del file. Nell'esempio seguente viene mostrato come aggiungere una riga per il servizio "syslog_monitor", configurato in modo da porsi in ascolto della porta TCP 5555.

   ```
   syslog_monitor5555/tcp
   ```

4. Modificare il file /etc/inetd.conf e aggiungere una voce per il nuovo servizio socket alla fine del file. Nell'esempio seguente viene mostrato come aggiungere una riga

per il servizio “syslog_monitor”, configurato in modo da eseguire lo script /usr/local/bin/in.syslog_monitor.

Inserire quanto segue in campi separati da tabulazioni in una sola riga del file, indipendentemente dalla modalità di visualizzazione.

```
syslog_monitor stream tcp nowait nobody
   /usr/local/bin/in.syslog_monitor in.syslog_monitor
```

5. Eseguire il comando seguente per attivare il processo del server socket:

```
kill -HUP `/bin/ps -ef | grep inetd | grep -v grep |
   awk '{print $2}'`
```

6. Collaudare il server socket. A tal fine, connettersi tramite Telnet alla porta desiderata per ricevere il contenuto del file di log:

```
% telnet localhost 5555
```

Per concludere la sessione Telnet, eseguire ^] (control-]) e digitare quit al prompt telnet>.